Data Center Certifications and Audits

Security Through Compliance

CyrusOne
Built for Tomorrow. Ready Today.

- ISO 27001
- TRUSTe
- Open-IX Association
- PCI DSS
- HIPAA
- FISMA
- SSAE 16

CyrusOne designs its facilities to comply with rigorous standards set by trade groups and certifying organizations, while maintaining relevant certifications and attestations.

The CyrusOne Compliance Management team is dedicated to continually improving and maintaining compliance certifications that are critical to our data center customers. Through disciplined assessment and audit processes, CyrusOne has implemented comprehensive practices for ISO/IEC 27001,SSAE 16 (SOC 1 Type II), Type 2 AT 101/SOC 2 & 3, PCI DSS, FISMA-High, HIPAA/HITECH, Business Continuity and Disaster Recovery (BCDR), and TRUSTe.

International Organization for Standardization (ISO 27001)

ISO 27001 defines specific controls that should be in place for an organization to be certified as in conformance with ISO 27001.

CyrusOne maintains ISO 27001 certification for operations of data centers in the United States. ISO 27001 is an International standard providing a model for establishing, operating, monitoring, and improving an Information Security Management System (ISMS.) The ISO 27001 Certification allows CyrusOne to demonstrate our commitment to information security processes.

The scope of data center colocation services covered includes physical controls, environmental safeguards, and telecommunication connectivity as well as support provided by CyrusOne's client service, legal/compliance, facility management and information technology departments.

TRUSTe – Privacy Certifications

CyrusOne has been awarded the TRUSTe Certified Privacy Seal after completing a Privacy Assessment and implementing the required changes. CyrusOne can proudly display the seal on all certified website, apps, and cloud/advertising platforms. TRUSTe is the #1 privacy brand and the Certified Privacy Seal is recognized globally by consumers, businesses, and regulators as demonstrating privacy best practices. CyrusOne's TRUSTe Policy can be found here. http://privacy.truste.

OPEN-IX

Open-IX Association

CyrusOne Data Centers have met and conformed to OIX standards, using systems and processes that have proved successful in our carrier neutral facilities since our founding in 2000. On January 21, 2014 it was announced that CyrusOne had become the first data center company to receive multiple data center OIX certifications.

Certification will act as the bedrock for a new and resilient interconnection marketplace in CyrusOne data centers allowing content and ISP's to have diverse locations for peering and transactional interconnection. This OIX accreditation enables a mutual model for interconnection that is the best for the future of the Internet. The OIX platform echoes the aims of the North American community as represented by the Open-IX initiative.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) was created to meet the rising threat to individuals' payment card information. Compliance with PCI DSS is mandatory for all organizations dealing with credit, debit and ATM cards, as defined by the PCI Security Standards Council, which includes industry giants like Visa, Master Card and American Express.

PCI DSS is a comprehensive set of standards requiring merchants and service providers that store, process, or transmit customer payment card data to adhere to strict information security controls and processes. The standard includes twelve requirements that include the following:

- Security management
- Policies and procedures
- Network architecture
- User access management
- Network and systems monitoring
- Software development.

CyrusOne provides physical security access to customer equipment through a combination of management systems and physical access safeguards and procedures. CyrusOne does not monitor or have access to customer data, so applicability is only to physical security and management processes that govern physical security.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) regulation impacts those in healthcare that exchange patient information electronically. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use or disclosure of the information.

HIPAA states a security management process must exist in order to protect against "attempted or successful unauthorized access, use, disclosure, modification, or interference with system operations."

HIPAA sets the standard for protecting sensitive patient data. Data centers must have certain administrative, physical and technical safeguards in place, according to the U.S. Department of Health and Human Services.

With colocation experts and secure facilities, staffed 24×7, CyrusOne can support your HIPAA compliance needs. CyrusOne meets required physical and administrative security controls, supporting your HIPAA physical security compliance through the following deliverables:

- Controlled Secure Facility
- 24/7 Physical Security Monitoring
- 90-Day Video Surveillance & Retention
- Cabinet/Cage Perimeter Security
- Badge and Biometrics
- Compliance Base Audit Reports
- Security Incident Response Notification.

Compliance is a shared responsibility. Your company must address, implement and manage all other technical and administrative controls outside of physical safeguards.

Federal Information Security Management Act (FISMA)

CyrusOne completed an independent security assessment of the information security controls outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 3 (SP 800-53.) NIST 800-53 outlines the controls that are required to comply with the Federal Information Security Management Act, or FISMA.

All government agencies, government contractors, and organizations that deal and exchange data with government systems must follow FISMA compliance guidelines. Organizations have to monitor, retain and maintain audit records of all security events as per FISMA (Federal Information Security Management Act).

The objective of FISMA compliance is to ensure that Federal departments and agencies observe measures to mitigate the security risks to critical data.

For federal agencies to use the services of a provider, the services must be based in a FISMA compliant data center that meets the stringent security requirements mandated by the Federal Information Security Management Act (FISMA). The National Institute of Standards and Technology (NIST) creates and maintains the specific security standards that agencies and their vendors are required to follow to remain compliant.

Agency compliance is ensured by the Office of Management and Budget (OMB), which each year reviews federal agencies' IT programs to verify that they are FISMA compliant whether hosted on- or off-premise. The scope of the assessment included CyrusOne's documented policies and procedures as well as controls implemented for its data centers. The controls that made up the assessment were awareness and training, incident response, maintenance, physical and environmental, personal security, and risk assessment.

SSAE 16
Type II Audited

SSAE 16 (SOC 1 Type II)

Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is attestation standards put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). This report is intended to be relied upon by the financial statement auditors of CyrusOne customers.

The SSAE 16 assesses the physical security, environmental safeguards and network monitoring controls implemented by CyrusOne. Assessing these controls through the SSAE 16 demonstrates CyrusOne's commitment to the protection of all IT assets.

Type 2 AT 101/SOC 2

Attestation Standard 101 (AT 101) are attestation standards put forth by the ASB of the AICPA that assess CyrusOne's controls against the Trust Services Principles and Criteria. The principles of Security and Availability are included in CyrusOne compliance reports.

SOC 2 reports in the CyrusOne's compliance suite includes test results of disaster recovery and business continuity plans. The availability of these services is a critical success factor for enterprise customers.

TIA MANUFACTURERS & SUPPLIERS OF GLOBAL NETWORKS

CyrusOne conducts independent analysis of all designs to ensure they meet the design criteria represented in the ANSI/TIA-942 standard, Rated-4: Fault Tolerant Site Infrastructure. ANSI/TIA-942 is a quality standard for data center that represents worldwide consensus from industry leaders on data center design and build.

Site Name	ISO 27001	SSAE 16	SOC 2	PCI DSS	HIPAA / HITECH	FISMA HIGH
Chandler - Ellis	Yes	Type 2	Type 2	Yes	Yes	Yes
Chandler - Ellis 4	Yes	Type 1	Type 1	Yes	Yes	Yes
Lombard - Springer	Yes	Type 2	Type 2	Yes	Yes	Yes
South Bend - Crescent	Yes	Type 2	Type 2	Yes	Yes	Yes
South Bend - Monroe	Yes	Type 2	Type 2	Yes	Yes	Yes
Florence - Industrial	Yes	Type 2	Type 2	Yes	Yes	Yes
Cincinnati - Goldcoast	Yes	Type 2	Type 2	Yes	Yes	Yes
Mason - Parkway	Yes	Type 2	Type 2	Yes	Yes	Yes
Cincinnati - 209 W 7th	Yes	Type 2	Type 2	Yes	Yes	Yes
Cincinnati - 229 W 7th	Yes	Type 2	Type 2	Yes	Yes	Yes
Hamilton - Knightsbridge	Yes	Type 2	Type 2	Yes	Yes	Yes
Lebanon - Kingsview	Yes	Type 2	Type 2	Yes	Yes	Yes
Austin - Ben White	Yes	Type 2	Type 2	Yes	Yes	Yes
Austin - Metropolis	Yes	Type 2	Type 2	Yes	Yes	Yes
Austin - Metropolis 3	Yes					
Carrollton - Frankford	Yes	Type 2	Type 2	Yes	Yes	Yes
Lewisville - Hwy 121	Yes	Type 2	Type 2	Yes	Yes	Yes
Houston - 5150 Westway	Yes	Type 2	Type 2	Yes	Yes	Yes
Houston - 5170 Westway	Yes	Type 2	Type 2	Yes	Yes	Yes
Houston - Southwest Fwy	Yes	Type 2	Type 2	Yes	Yes	Yes
Houston - Corporate Centre	Yes	Type 1	Type 1	Yes	Yes	Yes
San Antonio - 9999 Westover	Yes	Type 2	Type 2	Yes	Yes	Yes
San Antonio - 9554 Westover						
Sterling - Ridgetop Circle	Yes	Type 1	Type 1	Yes	Yes	Yes
Wappingers Falls - Myers Corners		Type 2	Type 2	Yes		
Totowa - Madison		Type 2	Type 2	Yes		
Stamford - Riverbend		Type 2	Type 2	Yes		
Norwalk - Norden		Type 2	Type 2	Yes		

To request a CyrusOne Compliance Report/Certification please contact customerservice@cyrusone.com.
Report copies can be provided upon request, subject to CyrusOne's Non-Disclosure Agreement (NDA).