Security Through Compliance

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

The Stream Data Centers Critical Environments Services practice is dedicated to continually improving and maintaining compliance certifications that are critical to our data center customers.

Through disciplined assessment and audit processes, Stream has implemented comprehensive practices for ISO/IEC 27001, PCI DSS, HIPAA/HITECH, FISMA-High, SSAE 18 (SOC 1 Type II), Type 2 AT 101/SOC 2, HITRUST and CSA STAR. Stream is also prepared to assist customers with obtaining their FEDRAMP certification.

ISO 27001

International Organization for Standardization (ISO/IEC 27001)

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

ISO 27001 is an International standard providing a model for establishing, operating, monitoring, and improving an Information Security Management System (ISMS.)

PCI DSS COMPLIANT

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, MasterCard 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 comprises twelve requirements, which include the following:

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

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

HIPPA
COMPLIANT

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 that 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, Stream Data Centers can support your HIPAA compliance needs. Stream Data Centers 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, and
- 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.

FISMA
COMPLIANT

Federal Information Security Management Act (FISMA)

Stream Data Centers 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 with 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-premises. The scope of the assessment included Stream Data Centers' 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.

SOC 2 (SSAE 18) TYPE II 80 101

Statement on Standards for Attestation Engagements (SSAE) are 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 Stream Data Centers customers. The SSAE assesses the physical security, environmental safeguards and network monitoring controls implemented by Stream Data Centers. Assessing these controls through the SSAE demonstrates Stream Data Centers' commitment to the protection of all IT assets.

Health Information Trust Alliance (HITRUST)

The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) is a comprehensive and certifiable security framework used by healthcare organizations and their business associates to efficiently approach regulatory compliance and risk management. HITRUST unifies recognized standards and regulator requirements from NIST, HIPAA/HITECH, ISO 27001, PCI DSS, FTC and COBIT, and can be completed according to SOC 2 criteria, making it the most widely adopted security framework in the U.S. healthcare industry.

CSA Security, Trust and Assurance Registry

CSA Security, Trust and Assurance Registry (CSA STAR) is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing and harmonization of standards, with continuous monitoring also available in late 2015. STAR certification provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings.

Stream Data Centers has been providing premium data center solutions and optimized value to Fortune 500 companies since 1999. To date, Stream has acquired and developed more than two million square feet of data center space in Texas, Minnesota, Illinois, California and Colorado, representing more than 200 megawatts of power.

Stream develops and operates highly resilient, scalable and efficient data centers. Stream's product offerings include fully-commissioned Hyperscale Data Centers, Private Data Center™ Suites, Ready-to-Fit™ Powered Shells, Build-to-Suit Infrastructure and Retail Colocation Environments – all with immediate connection to network carriers and public cloud providers.