Through disciplined assessment and audit processes, Stream has implemented comprehensive practices for ISO/IEC 27001, PCI DSS, SOC 1 (SSAE 18) TYPE II, and SOC 2 (SSAE 18) TYPE II.

Our team ensures compliance through:

- **Audit readiness** — Others in the industry may relax stringent attention to compliance until the last quarter, then tighten control to prepare for end-of-year audits. Stream's philosophy is that we should be audit-ready every day. We maintain our books, processes, training, STEPS program and CETA program to make sure we are.

- **Self-auditing** — We take compliance seriously, and continually self-audit in the areas of health and safety, processes and procedures. Managers frequently conduct informal audits of different areas, like safety and efficiency, to see how processes are working. Conscious self-auditing reinforces our commitment to compliance in the minds of our team. We don't require third parties or official audits to keep us up to standard.

- **Transparency** — Our partners are always welcome to visit our sites to meet the team and ask questions. Often, a visiting partner will choose a topic from STEPS to review with the on-site team. Stream operates with trust and integrity on every level.

- **Financial accountability** — Stream's commitment to compliance, process management and teamwork brings value to customers and supports profitability. We believe financial success is a byproduct of having the right team doing the right job the right way. And our profits go toward improvement, innovation, and strengthening the team as needed.
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.)

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.

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.

SOC 1 (SSAE 18) TYPE II
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 SOC 1 assesses the effectiveness of business process controls, physical access controls and logical access controls related to the property management administrative services performed for Stream Data Centers clients.

SOC 2 (SSAE 18) TYPE II
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.