

Hitachi Vantara Statement on Post-Quantum Cryptography (PQC) Readiness

Hitachi Vantara is committed to developing secure solutions that address the evolving cybersecurity landscape. As quantum computing capabilities continue to advance, Hitachi Vantara is monitoring developments in Post-Quantum Cryptography (PQC), including emerging laws, regulations, standards, and industry guidance. Our approach includes evaluating relevant PQC algorithms and their potential use in key exchange and digital signature mechanisms within established protocols such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec), where appropriate. This work is intended to support alignment with applicable requirements and help customers understand our approach to cryptographic readiness as the ecosystem continues to mature.

Many Hitachi Vantara solutions support data-at-rest encryption capabilities, including the Advanced Encryption Standard with 256-bit keys (AES-256), where applicable. AES-256 is widely recognized as a strong encryption method and can continue to support data protection strategies as organizations prepare for the quantum era. At the same time, Hitachi Vantara recognizes that broader post-quantum readiness requires continued evaluation of cryptographic technologies, standards, and implementation guidance. As new PQC standards and recommendations evolve, Hitachi Vantara will continue assessing their relevance to applicable products, protocols, and security capabilities.