Quantum®

Data Privacy and Security Statement

February 2018

The rising frequency of data breaches, and continued implementation of data privacy and security standards and regulations mean data users and managers are increasingly concerned about the compliance features of technology products. These standards and regulations generally allow for architectural independence so that technology infrastructures may evolve with innovation and flexibility to reflect unique environments and needs. Regardless of the technology solutions deployed, data controllers and others building data storage infrastructures are charged with maintaining appropriate technical, administrative, and physical controls to protect the privacy and security of their data, wherever that data is located.

Quantum products employ a number of technical, administrative, media protection, access, and other security controls that enable customers to design and implement storage infrastructures containing the system safeguards required to remain compliant with applicable guidelines and restrictions. More specific information about product features is available from your Quantum product team.

Ultimately, Quantum products are designed to operate within the configurations our customers set for them. It is incumbent upon customers (particularly those concerned about cross-boundary data transfers) to determine how to deploy product features and controls to ensure their data storage practices and environments, including other systems and technologies that might interact with Quantum products, are capable of meeting their compliance needs.

Quantum encourages customers to routinely review the feature and control configurations they have implemented in Quantum products, and throughout their broader IT environments, to evaluate their ability to address their ongoing data privacy and security requirements.

Quantum®

EC00027A-v01