

Meeting PCI DSS compliance requirements demands a more evolved enterprise solution.

Whether you are a service provider or merchant, it is the nature of your business to handle consumer credit and debit card information. And, regardless of your organization's size, handling this information requires compliance with the Payment Card Industry Data Security Standard (PCI DSS). You need a solution that can help meet compliance requirements, but also ensure that your data is completely secure throughout the data transfer and storage process.



SecureZIP®

FEATURES & BENEFITS

Exceed compliance requirements.

Securely exchange consumer credit & debit card information/files to meet PCI DSS compliance requirements.

Strongly encrypt sensitive data.

Use strong encryption to protect Primary Account Numbers (PANs) and other PII to ensure it is unreadable if lost or stolen.

Protect data in storage.

Ensure the security of data regardless of where it is stored or for what length of time.

Protect data in transit.

Data is protected, regardless of transmission method or destination platform.

Enforce organizational security policies.

Protect sensitive information according to your internal policies, even when information travels outside the organization.

Secure sensitive information *and* meet PCI DSS compliance requirements.

SecureZIP ensures that sensitive customer data remains secure within your organization's network as it travels from user to user and platform to platform. And, because of its data-centric approach to security, meeting specific requirements of PCI DSS is easy. Sensitive information is secure. Compliance requirements are met.

Your unique challenges

Requirement 3 of PCI DSS states that data should be protected.

Requirement 3.4 states that a PAN should be rendered "at a minimum, unreadable anywhere it is stored." It emphasizes that encryption is a critical component of cardholder data protection and that strong cryptography with key management is recommended.

Requirement 4.1 states that strong cryptography should be used to "safeguard sensitive cardholder data during transmission over open, public networks."

Requirement 4.2 states that cardholder information should never be sent in unencrypted email.

Requirement 7 states that organizations should "restrict access to data by business need-to-know."

Our unique solutions

SecureZIP encrypts and decrypts information using X.509 digital certificates, passphrases, or both. The integration of ZIP compression with strong security not only ensures that information is secure, but it enables portability and efficient exchange of information across all major enterprise computing platforms.

SecureZIP uses data-centric security to ensure even the most sensitive information can be sent via open, public networks without additional layers of protection. AES strong encryption, up to 256-bit, exceeds PCI DSS requirements. Information can also be sent via email, as messages and attachments can be encrypted to ensure cardholder information remains protected.

SecureZIP can restrict access to data at the server/application level by enforcing internal data security policies. In addition, it can prevent access to data at the file level by applying strong encryption to ensure it is only accessible by authorized individuals.

PKWARE®

www.pkware.com

Take the next step.

As volumes of data continue to multiply and compliance regulations become more stringent, you need a solution that solves the challenges you're facing today and those you'll face tomorrow. **Contact us today.**

Today, over 30,000 customers worldwide use SecureZIP solutions to optimize the management and protection of their data, as well as access to critical information. PKWARE's philosophy is to help solve the critical business challenges our customers are facing, while conserving valuable resources and maximizing their return on investment.



Meet PCI DSS Compliance Requirements; Avoid Liability Risk due to Data Loss or Theft

A data security breach could lead to irreparable damage to your reputation and revenue. SecureZIP helps avoid the costs, legal penalties, and damaged reputations that can be caused by compromised data. SecureZIP integrates naturally into existing workflows and provides end-to-end data protection, ensuring sensitive information is always protected both inside and outside your organization. In addition, SecureZIP can further increase email security by leveraging existing Public Key Infrastructure (PKI) for secure email exchange using X.509 digital certificates and digital signatures.



Meet PCI DSS Compliance Requirements; Protect Information Exchanged with External Partners

Daily business activities require information to be exchanged outside the perimeter of your organization. Huge amounts of data need to be transferred to various external partners without the risk of it being lost, stolen, or exposed once it leaves your network. SecureZIP PartnerLink works across all major enterprise computing platforms, enabling secure data exchange with a multitude of external endpoints. And, it is available to partners at no cost, accelerating deployment and acceptance. Information is seamlessly and securely exchanged with external partners without impacting their budgets.



Meet PCI DSS Compliance Requirements; Protect Information during Transfer, in Storage, and on Removable Media

In order to efficiently and effectively respond to business needs, large amounts of potentially sensitive data are exchanged frequently within an organization. SecureZIP's data-centric approach to security ensures that strong encryption is applied to the data and remains with it in storage and during all steps of the transfer process. In addition, information placed on removable media, including CDs, tapes, and USB drives also remains protected, even if lost or stolen. Reducing file size using ZIP compression and adding strong encryption ensures that information can be moved securely and efficiently.



Meet PCI DSS Compliance Requirements; Reduce Data Center Costs & Operational Overhead

It is easy to become trapped between the critical need for data security and the additional costs and operational burdens traditionally associated with it. By combining ZIP compression with strong encryption, SecureZIP not only ensures information is secure, it also enables portability and efficient exchange of information across all major enterprise computing platforms. In addition, SecureZIP maximizes the infrastructure investments you've already made to deliver a solution that works throughout your organization quickly and effectively.