






< Previous


















Next >

### Encrypt data

 Bookmark this page

Data security plans should require the use of strong encryption for sensitive data. Strong encryption is generally considered to include 128 or 256 bit ciphers available in a variety of forms, including "GnuPG." Data should be stored and communicated in encrypted form. When external parties are used for data storage purposes, the data should be encrypted before being passed to those parties, even if they can provide encryption services. We have learned that the NSA and law enforcement authorities commonly require providers of data storage and communications services to provide them with encryption keys and other information necessary to decrypt targeted data.

< Previous

Next >

© All Rights Reserved

