Laptop Security

All FDIC laptops are protected with full-disk encryption (FDE) to prevent sensitive data being taken from a laptop that has been lost, stolen, or left unattended. The entire laptop hard drive is automatically encrypted with no user action to secure all data on the hard drive.

The encryption uses Advanced Encryption Standard 256-bit key algorithms for a strong encryption mechanism. Logical partitions are boot-protected and encrypted sector-by-sector. Attempts to copy individual files or to introduce rogue programs are blocked, even when the hard drive is removed and slaved to a different computer. This encryption standard is Federal Information Processing Standard 140-2 compliant, which is a U.S. government computer security standard used to accredit cryptographic modules employed within federal IT space.

Complementing the use of FDE software, all users must use multifactor authentication to log into the laptop. Configuration settings are in place to automatically lock the FDIC laptop after 15 minutes of inactivity, requiring the user to re-authenticate before access to the laptop is granted. Consecutive incorrect login attempts will lock the laptop and require the assistance of an authorized FDIC administrator to regain access.

All FDIC laptops are prevented from writing to external devices like USB or CD/DVD. Accesses to Internet webmail and file share websites are blocked.

Secure E-mail security

Zix is an FDIC Secure E-mail Service which allows FDIC employees to communicate confidential and sensitive business information through a secure channel with individuals outside the FDIC (external users only). Once the message is sent from FDIC, the external user then retrieves the message from the FDIC Secure Email Message Center, a secured website. The recipient's reply to this message is automatically encrypted and returned directly to an FDIC employee’s email inbox.

FDICconnect –Enterprise File Exchange (EFX)

Data exchanged via EFX is securely maintained in FDIC information systems rated at the Federal Information Security Management Act (FISMA) “moderate” risk level. To protect these systems, the FDIC uses a defense in depth approach supported by an alignment to the National Institute of Standards and Technology Cybersecurity Framework, FISMA requirements, and FDIC-wide directives that guide the operations, roles and responsibilities of employees and contractors.

Bank Data Purge from FDIC Systems

Bank data received by the FDIC for the purpose of the compliance review will be purged entirely from FDIC systems after the review is completed. This includes raw data files, intermediate data files, and database tables. The FDIC will notify the bank in writing when the data has been deleted.