Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

This publication specifies the Triple Data Encryption Algorithm (TDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA). When implemented in an SP 800-38-series-compliant mode of operation and in a FIPS 140-2-compliant cryptographic module, TDEA may be used by federal organizations to protect sensitive unclassified data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data.

This recommendation defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data. TDEA is made available for use by federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls.

Use this recommendation from the National Institute of Standards and Technology (NIST) to protect your organization's sensitive data.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- Recommendation for the Triple Data Encryption Algorithm Block Cipher.pdf