STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 Silver Lake Blvd.
Dover, Delaware 19904

Doc Ref Number:	SE-KEY-001	**Revision Number:** 0
Document Type:	Enterprise Policy	**Page:** 1 of 6
Policy Title:	Encryption Key Management Policy	

Synopsis:	This policy provides ways to securely handle encryption keys in order to avoid the loss of data in State of Delaware organizations.		
Authority:	Title 29 Chapter 90C Delaware Code, §9004C – General Powers, duties and functions of DTI "2) Create, implement and enforce statewide and agency technology solutions, policies, standards and guidelines, including as recommended by the Technology Investment Council on an ongoing basis and the CIO"		
Applicability:	This Policy is applicable to all users of the State of Delaware communications and computing resources. DTI is an Executive Branch Agency and has no authority over the customers in Legislative and Judicial Branches, as well as School Districts, and other Federal and Local Government entities that use these resources. However, all users, including these entities, must agree to abide by all policies, standards promulgated by DTI as a condition of access and continued use of these resources.		
Effective Date:	9/29/2009	**Expiration Date:**	None
POC for Changes:	Solomon Adote, Chief Security Officer		
Approval By:	Secretary Jim Sills, Chief Information Officer		
Approved On:	9/29/2009		

TABLE OF CONTENTS

I. Policy

EXECUTIVE SUMMARY
Encryption key management is a crucial part of any data encryption strategy. A failure in encryption key management can result in the loss of sensitive data and can lead to severe penalties and legal liability.

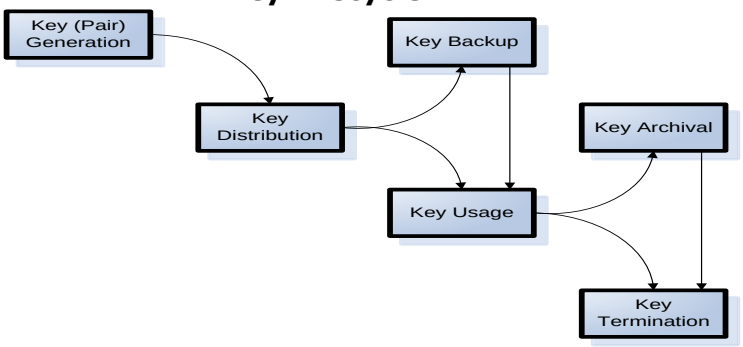
PURPOSE
This policy will set forth the minimum key management requirements.

POLICY STATEMENT

- Data classification of keys – The classification of symmetric and private keys inherits the classification of the data that it is securing. The minimum classification is confidential.

- Key access – Keys must be protected such that only authorized users and applications can access the keys. The keys used to encrypt data should not be stored on the same media as that data. Whenever keys are stored either physically or logically in close proximity to the data that it is protecting mitigating controls must be in place to ensure a compromise of the data does not happen. Such mitigating controls must include, but are not limited to, the encryption of the keys themselves.
- DR testing – Routine testing of key recovery should be based on the DR/BC plan associated with the system.
- Audit reporting requirements – Usage of keys must be logged to provide an audit trail.
- Cryptoperiod of the key – The lifetime of the key must be commensurate with the strength of the key and the data classification of the data that the key is used to encrypt. It is the agency's responsibility to define and adhere to the cryptoperiod.
- Key Lifecycle: The lifecycle of the key can be summarized as generation, distribution, storage, usage, restoration (if necessary), and termination. The following diagram and bullets will elaborate on these phases and outline requirements whenever applicable.

Key Lifecycle



1. Key generation methods – Keys must be generated by cryptographic algorithms approved by DTI.
2. Key distribution and transportation – Private and symmetric key distribution must be handled securely such as secure email or out of band techniques like phone conversations with known individuals. Physical transportation of private and symmetric keys will require that they will be encrypted.
3. Key backup – Keys used for encrypting 'data at rest' must be backed up with documented and proven recovery processes in place.
4. Key usage – Unique keys (or asymmetric key pairs) should be used for distinct cryptographic processes. Reusing the same keys for different processes may weaken the security provided by one or both of the processes.
5. Key archival – The integrity and access to the keys must be preserved during the retention period, which often requires the preservation of the software and hardware modules used in the encryption process.
6. Key retention– Keys must be retained according to the data retention schedule governing the data that those keys are used to encrypt.
7. Key termination – Symmetric and private keys must be securely erased.

IMPLEMENTATION RESPONSIBILITY

DTI and/or the organization's technical staff will implement this policy during the course of normal business activities, including project execution and the design, development, or support of systems.

ENFORCEMENT and WAIVER

DTI will enforce this policy during the course of normal business activities, including review of proposed projects and during the design, development, or support of systems. This policy may also be enforced by others during the course of their normal business activities, including audits and design reviews.

If there is ambiguity or confusion regarding any part of this policy, contact the point of contact defined in the header of this policy.

II. Definitions

Algorithm – A procedure or formula for solving a problem. The word derives from the name of the mathematician, Mohammed ibn-Musa al-Khwarizmi, who was part of the royal court in Baghdad and who lived from about 780 to 850. Al-Khwarizmi's work is the likely source for the word *algebra* as well.[1]

Asymmetric-key algorithm –
http://en.wikipedia.org/wiki/Public_key_cryptography

Cipher – A cipher is any method of encrypting text (concealing its readability and meaning). It is also sometimes used to refer to the encrypted text message itself although here the term ciphertext is preferred.[2]

Ciphertext - Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.[3]

Cryptoperiod - A cryptoperiod is a specific time span during which a cryptographic key setting remains in effect. A key uses an algorithm to create ciphertext from plaintext and, for the receiver of the encrypted text, to decipher it. Once the cryptoperiod ends, the key is no longer available for either encryption or decryption.[4]

Decryption - the process of converting encrypted data back into its original form, so it can be understood.[5]

[1] http://whatis.techtarget.com/definition/0,,sid9_gci211545,00.html
[2] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213593,00.html
[3] http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci213853,00.html
[4] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci518928,00.html
[5] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html

Encryption - The conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.[6]

Key – In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.[7]

Plaintext - Ordinary readable text before being encrypted into ciphertext or after being decrypted.[8]

Symmetric-key algorithms – http://en.wikipedia.org/wiki/Symmetric-key_algorithm

[6] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html
[7] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213695,00.html
[8] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213596,00.html

III. Development and Revision History

Initial version established **9/29/2009**

IV. Approval Signature Block

Name & Title: Cabinet Secretary - State Chief Information Officer	**Date**

V. Listing of Appendices

SP 800-57 Part 1 – Recommendation for Key Management – Part 1: General (Revised)
SP 800-57 Part 2 - Recommendation for Key Management – Part 2: Best Practices for Key Management Organization
SP 800-57 Part 3 - DRAFT Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance SP 800-57 Part 3