The Universities
AT SHADY GROVE

Encryption Policy

USG Policy 6 (2.20) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to outline USG's standards for use of encryption technology in order to properly secure and manage appropriately its data assets. There are additional USG security policies that reference the types of data that require encryption. This policy does not cover what types of data must be encrypted, but rather how encryption is to be implemented and controlled.

The scope of this policy covers all data stored on or transmitted across USG-owned, USG-managed, and USG-leased systems, devices, media, and networks. This policy also applies to all USG hired personnel, contractors, and third-party services.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as “OIT.” This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Encryption:* the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

B. *Encryption Key:* an alphanumeric series of characters that enables data to be encrypted and decrypted.

C. *Password/Passphrase:* a sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

D. *Public Key Encryption (Asymmetric):* an encryption technique that uses a key pair composed of a public key and private key. Best used for digital signatures, SSL certificates, authentication, and more due to slow performance, but ease of key distribution.

E. *Private Key Encryption (Symmetric):* an encryption technique that only uses one secret or privately held key. Best used for encryption of data in transit due to performance considerations.

III. Encryption Minimum Standards

A. USG requires the use of all encryption algorithms and standards to, at a minimum, comply with the following:

1. NIST Special Publication 800-175B (*"Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms"*)
2. Federal Information Processing Standards (FIPS) Publication 140-2 *("Security Requirements for Cryptographic Modules"),*
3. Or any other superseding publication, regulation, or USM/State of Maryland policy

B. The use of proprietary encryption is expressly forbidden since it has not been subjected to public inspection and its security cannot be assured.

IV. Encryption Key Management

The following guidelines apply to USG's Public Key Infrastructure (PKI):

A. Certificates

1. All certificates should be issued by an authorized Certificate Authority (CA); self-signed certificates are strongly discouraged.
2. All certificates must be maintained in a central repository to preserve availability of keys for use in decryption of encrypted data and digital signatures.
3. All certificates must have an expiration date and process established for validation and revocation, such as a published Certificate Revocation List (CRL).
4. All issued certificates must be properly assigned to a user or server by a qualified name within an authorized PKI.
5. All issued certificates must be associated with an active service or function.

B. Private Keys

1. USG strongly encourages that private keys should be backed up to maintain availability to associated encrypted data.
2. Private keys must always be encrypted in transit.
3. Private keys should never be shared

C. The following guidelines apply to all symmetric (private/pre-shared) key encryption:

1. USG strongly encourages that all keys should be backed up to maintain availability to associated encrypted data.
2. All keys must always be encrypted in transit.
3. All passphrases must always be encrypted in transit and only be shared with authorized staff and associate/partners of USG.
4. All passphrases should comply with password guidelines outlined in the latest USM IT Security Standards on Access Control Standards.

V. Encryption Sustainability

A. The Office of Information Technology (OIT) at USG must outline and implement a transition/recovery process where OIT has the ability to recover and constantly maintain encryption for all previously encrypted data during either a changeover in personnel or unintended loss/destruction of an encryption key.

VI. Legal Uses of Encryption

A. When the use of encryption technology is applied, USG personnel must always abide by and conform to Federal, State, and Local government regulations during the use and import/export of encryption technologies. USG specifically forbids the use of encryption to hide illegal, immoral, or unethical acts.

VII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

VIII. Revision History

Date	Description	Revised By
01/23/2018	Initial Policy Creation	Russell Schlosburg

IX. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

B. NIST FIPS 140-2
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

C. NIST SP800-175B
http://dx.doi.org/10.6028/NIST.SP.800-175B