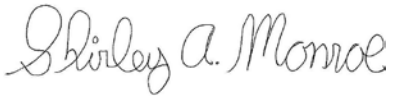
COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Bitlocker Standard**	Number: **STD-SAS001**
Domain: **Security**	Category:
Date Issued: **12/05/11**	Issued By Direction Of:  Shirley A. Monroe, Dir of Div of Technical Engineering
Date Revised: **08/28/13**	

Abstract:
The purpose of this Security standard is to improve the confidentiality and integrity of data at rest by requiring the use of Full Disk Encryption on all DPW, PID, Agings Windows 7 desktops and Laptops by using BitLocker.

- **Full Disk Encryption**:
  Full disk encryption is a computer security technique that encrypts data stored on a mass storage or removable device, and automatically decrypts the information when an authorized user requests it. Full disk encryption is often used to signify that everything on a disk or removable device, including the operating system and other executables, is encrypted. Windows 7 comes with BitLocker built in which will give the three agencies the ability to increase security by leveraging the Full Disk Encryption built into the operations system of Windows 7.

Objective:
This standard requires all DPW, PID and Aging desktops to use Full Disk Encryption built into Windows 7.

Scope:
This standard is applicable to DPW, PID, Aging employees, contractors, business partners.

Policy:
DPW, PID and Aging store sensitive data such as PII (Personal Identifiable Information) and PHI (Personal Health Information) which it is the responsibility of the three agencies to protect that data from unauthorized use. With desktops being upgraded to Windows 7, BitLocker will provide Full Disk Encryption which will help protect any stored data located on the Agencies PCs.

Additionally, agencies must ensure that any non-commonwealth entity or agency business partner/contractor which stores or has access to such data also protects stored sensitive, protected through the use of encryption.

BitLocker Full Disk Encryption:

BitLocker Drive Encryption to help protect all files stored on the drive Windows is installed on (operating system drive) and on fixed data drives (such as internal hard drives). When you add new files to a drive that is encrypted with BitLocker, BitLocker encrypts them automatically. Files remain encrypted only while they are stored in the encrypted drive. Files copied to another drive or computer is decrypted. If you share files with other users, such as through a network, these files are encrypted while stored on the encrypted drive, but they can be accessed normally by authorized users.

The BitLocker Drive Encryption operates in conjunction with cryptographic modules of the Vista operating system. The following cryptographic algorithms are used as part of the BitLocker modules:

- Hashing: SHA-1 (for TPM communications), SHA-256
- Keyed hash: HMAC, AES in CCM mode (128 and 256 bit)
- Symmetric key encryption: AES in CBC mode (128 and 256 bit), with or without the use of the Elephant Diffuser algorithm

Exemptions from this Standard:

Any Program Office that is unable to comply with this standard must discuss any exemption request with the Department's CISO (Chief Information Security Officer).

Refresh Schedule:

All standard and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by DPW Information Technology Standards Team.

Standard Supplements:

None

References:

1. BitLocker Drive Encryption Security Policy - FIPS 140-2 Validation

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
12/05/11	1.0	Created BitLocker standard	Tom Zarb, BIS/DTE/SAS
08/28/13	1.1	Reviewed Content and formatted	Mathieu Saury