# Encryption Standard

## Related Policy

* 201.00 Asset and Data Protection Policy

## Purpose

The purpose of the Encryption Standard is to build on the principles established in the Asset and Data Protection Policy to provide the requirements for use of encryption technology so that HBI or MBI information as defined in the Data Security Classification Standard is appropriately protected and encryption technologies are used and managed appropriately.

## Standard Statements

### When to Use Encryption

* 1. There are six primary conditions when sensitive information must be protected by using encryption:
     1. When hosting or implementing web pages which contain HBI or MBI as defined in the Data Security Classification Standard.
     2. When using an external network (for example, the internet or public Wi-Fi) or a third party network to exchange data which is classified as HBI or MBI as defined in the Data Security Classification Standard.
     3. When using the internal Alight network to exchange data which is classified as HBI (for example, personal data) as defined in the Data Security Classification Standard.
     4. When storing HBI or MBI data within a database, file server or bulk storage device.
     5. When making a back-up copy of HBI or MBI data.
     6. When holding data on portable media / devices (such as laptops, mobile devices, USB devices, etc.).

### Transmission

* 1. Implement transmission controls in accordance with the Data Security Classification Standard.
     1. Encrypt information transmitted between remote locations and the Alight networks.
     2. Encrypt all data transmitted through wireless communications.
     3. Encrypt remote administration sessions.

### Storage

* 1. Implement storage controls in accordance with the Data Security Classification Standard.
     1. If full disk encryption is used, manage logical access to a fully encrypted disk separately from access to the native operating system.
     2. Store decryption keys separately from the encrypted volumes they are protecting.
     3. Encrypt mobile or removable media devices.

### Approved Encryption Algorithms

Encryption of data must use an approved encryption algorithm, as defined in this section. Encryption must also meet any specific statutory, regulatory, or client algorithm requirements, when specified. When multiple statutory, regulatory, or client encryption algorithm requirements are applicable, the most secure of the encryption algorithms specified must be used. Use of encryption algorithms that are not approved by Alight’s Global Security Services is prohibited.

* 1. Approved Symmetric Encryption Algorithms

|  |  |
| --- | --- |
| Symmetric Encryption Algorithms | Comments |
| AES | Key length: 256 bits or higher. |
| 3DES | Do not use in new applications. |

* 1. Approved Asymmetric Encryption Algorithms

|  |  |
| --- | --- |
| Asymmetric Encryption Algorithms | Comments |
| RSA | Key length: 2048 bits or higher as technologies allow. |
| ECC | Use the prime and binary field recommendations from NIST, FIPS PUB 186-4, ([Digital Signature Standard,DSS)](http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf) |

* 1. Approved Cryptosystems

|  |  |
| --- | --- |
| Cryptosystems | Comments |
| Kerberos | Use version 5 or higher |
| SSL | No longer acceptable for use. |
| TLS | Use TLS 1.1 or higher |
| OpenPGP |  |
| WPA2 | Use Enterprise version; Reference wireless security standard |
| SSH | Use version 2 |
| S/MIME |  |
| IPSec |  |
| Public Key Cryptographic System | Public Key Cryptography Standard (PKCS), Version 2.2 |
| Digital Certificate | X.509 v3 certificate;  X.509 v2 certificate revocation list (CRL) |
| Cryptographic Module Assurance | Federal Information Processing Standards Publication 140-2 Level 2 or higher |

* 1. Approved Hashing Algorithms

|  |  |
| --- | --- |
| Hashing Algorithms | Comments |
| MD-5 | No longer acceptable for use. Use SHA-3 hashes. |
| SHA-2 | SHA-2 hashes are approved for legacy applications.  Where possible, developers must stop using SHA-2 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-3 family of hash algorithms for these applications. |
| SHA-3 | Use the SHA3 family of hash algorithms for digital signatures, digital time stamping and other applications that require collision resistance. |
| HMAC | Since the cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, use a hash from the SHA-3 family of hashing algorithms. |

### Key Management

* 1. Document and implement procedures for key management, including administration, access, key generation, distribution, storage, re-keying, and destruction of keys.
  2. Key custodians must understand components of this standard and accept their responsibilities.
  3. All root keys must have dual custodians with split key knowledge so that no single custodian has access or full knowledge of the key value.
  4. Users must safeguard their data encryption keys, private keys, passphrases, and/or digital certificates entrusted to them.
     1. Private keys are not permitted to be printed out.  Any files containing a user's encryption key(s) must be encrypted.
     2. Passwords and public keys required for encryption and decryption must be transmitted separately from information encrypted using the key.
     3. All encryption hardware, software, and keys must be classified as Alight Highly Confidential – High Business Impact.
  5. All general-purpose file and E-Mail encryption processes running on Alight computers must include centralized encryption key recovery functions. Access to server directories containing cryptographic keys must follow least privilege principle.
  6. Only Alight-issued or approved vendor purchased cryptographic keys must be used for Alight business purposes or to protect sensitive information.
  7. Replace known or suspected compromised keys immediately.
  8. Archive keys for the life of encrypted information and the corresponding need to decrypt.

### Export Controls

* 1. Export Controls:  Users must comply with their national encryption export regulations.  Alight managers must coordinate with Global Security Services when encryption products are being considered for use outside of the countries designated by the Wassenaar arrangement.  It is prohibited to transmit, in any manner, software containing export-restricted encryption technology outside of the Wassenaar designated countries.

## References and Mandates

* None

## Legal Conflicts

Alight Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard of Alight shall take precedence over the more general provisions contained in Alight Security Policies and Standards.

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | INFOSEC\_201.03 Encryption Standard |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.6 |
| Owner | Alight Global Security Services | Information Security |
| Author(s) | Alight Global Security Services | Information Security |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 2, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

# Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 March | Original | Restructured due to Aon Hewitt merger |
| 1.1 | 2012 September | Update | Updated Section 4 with approved encryption and hashing algorithms and crypto systems |
| 1.2 | 2013 June | 2013 Annual Review | Reviewed and validated  1.1.5: clarified the intent of the statement.  4.4: Changed should to must |
| 1.3 | 2014 June | 2014 Annual Review | Reviewed and validated  4.1: Clarified that encryption labeled as RC6 compliant is also acceptable  4.4: Added SHA3 as the more desirable hashing standard. |
| 1.4 | 2015 June | 2015 Annual Review | Reviewed and validated – add Legal Conflicts |
| 1.5 | 2016 August | 2016 Annual Review | Clarified use cases and updated list of approved encryption algorithms and systems. |
| 1.6 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |