IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Security Standard – Use of Cryptography (SS-007)

Chief Security Office

Date: 12 April 2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

1. Introduction

1.1. This cryptographic security standard provides the list of controls that are required to secure implementations of cryptography to a DWP approved level of security. It is to minimise the risk from known threats, both physical and logical, to an acceptable level for operational consumption.

1.2. Associated key management requirements are not detailed in this standard and instead can be found in SS-002 Security Standard – Public Key Infrastructure.

1.3. For further clarity and relevance, this standard is aligned the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.4. Furthermore, the security controls presented in this standard have been taken from international best practice, recommendations made by trusted government agencies such as the National Cyber Security Centre (NCSC) and well-evidenced academic findings.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for cryptographic deployments.

2.2. Secondly, this standard provides a means to conduct compliance-based technical security audits and IT Health Checks.

3. Exceptions

3.1. In this document the term “MUST” in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption as detailed below.

3.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.3. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the controls detailed in this standard.

3.4. Exceptions to this standard MUST be maintained on the project’s risk register for accountability, traceability and security governance reporting to senior management.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

4. Audience

4.1. This standard is intended for consumption by technical architects, software engineers, developers and security staff. It should be consulted in the design, assurance and audit of cryptographic systems (cryptosystems) deployed within DWP.

5. Scope

5.1. This standard is to cover cryptographic systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP), including the handling caveat OFFICIAL-SENSITIVE. All of the organisation's cryptographic systems (cryptosystems) falling within this category will be subject to the requirements specified within this security standard. The requirements will be applicable to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all cryptographic systems that are provisioned for departmental use.

5.3. In the event of uncertainty on the controls laid out in this standard, please contact the Security Front Door for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7. Technical Security Control Requirements

In the section below, a term written in *italic text* indicates that a definition of the term can be found in Definition of Terms.

7.1 Software and Hardware Requirements

Reference	Security Control Requirement
10.1.1	*Cryptographic software* MUST achieve a minimum of *FIPS 140-2* Level 1 certification or alternatively certification provided by the National Cyber Security Centre (e.g. Commercial Product Assurance (CPA)).
10.1.2	*Cryptographic software* MUST be updated in adherence to DWP patching policy.
10.1.3	*Cryptographic hardware* MUST achieve a minimum of *FIPS 140-2* Level 2 certification or alternatively certification provided by the National Cyber Security Centre (e.g. Commercial Product Assurance (CPA)).
10.1.4	*Cryptographic software* and *cryptographic hardware* MUST be deployed and configured in accordance with the terms and conditions associated with its certification or approval.
10.1.5	*Cryptographic software* and *cryptographic hardware* MUST only be used when still under active vendor support.

7.2. Cryptographic Algorithm Requirements

Reference	Security Control Requirement
10.2.1	*Cryptographic algorithms* and *modes of operation* MUST be selected from the latest approved version of the DWP Approved Cryptographic Algorithms document. Where multiple algorithms are deployed, the order of preference given by this document MUST also be technically enforced.
10.2.2	The list of approved *cryptographic algorithms* MUST be reviewed at least annually.
10.2.3	Approved asymmetric cryptography MUST only be used: a) To negotiate or exchange secrets for symmetric cryptography; b) To create and verify digital signatures; c) To encrypt data where symmetric cryptography is inappropriate.
10.2.4	Approved cryptographic hashing algorithms MUST be used as the basis for: a) Creating message digests; b) Generating digital signatures; c) Message Authentication Codes (MACs / HMACs); d) Pseudorandom Functions (PRFs); e) Key Derivation Functions (KDFs).
10.2.5	Where information is to be encrypted and authenticated, the Message Authentication Code (MAC) MUST be computed after encryption (i.e. *encrypt-then-MAC*).
10.2.6	Elliptic Curve Cryptography (ECC) curves and key parameters MUST be selected from those recommended in FIPS 186-4 Appendix D, Sections D.1.2 and D.1.3.
10.2.7	The Diffie-Hellman (DH) key exchange algorithm MUST be used in conjunction with the following parameters: a) Diffie-Hellman Group 14; or b) Diffie-Hellman Group 15; or c) Diffie-Hellman Group 16; or d) Self-generated pseudorandom parameters of 2048 bits in length (or greater).

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7.3 Generation of Cryptographic Key Material

Reference	Security Control Requirement
10.3.1	If not already implemented within approved software, *pseudorandom data* generated for the purpose of improving the security of a system (including initialisation vectors) MUST use cryptographically secure sources of entropy. Acceptable sources are: a) External modules which have received National Cyber Security Centre Commercial Product Assurance (CPA) certification, *FIPS 140-2* certification, or NIST SP 800-90 certification; b) Operating system certified sources (e.g. Microsoft CryptoAPI-NG, /dev/random).
10.3.2	Virtual Machines (VMs) and operating systems running on Solid State Drives (SSDs) MUST only be used in the generation of cryptographic *pseudorandom data* (e.g. keys, IVs) where the lifetime of the cryptographic data is 48 hours or less; except in the case where an external module described in Clause 10.3.1a) is deployed.

7.4 Compression

Reference	Security Control Requirement
10.4.1	Compression of data MUST be a separate process to the encryption and decryption operations themselves. Compression routines that execute alongside encryption and decryption functions (e.g. TLS compression) are prohibited.

7.5 Message Padding

Reference	Security Control Requirement
10.5.1	Messages to be encrypted by an approved asymmetric algorithm MUST avoid using PKCS#1 v1.5 padding.

7.6 Encryption in Transit

Reference	Security Control Requirement
10.6.1	Encrypted communication transiting DWP-owned or –managed infrastructure MUST be designed to support content inspection capabilities as part of the security boundary inspection policy.
10.6.2	Encrypted communications channels MUST be protected using one of the following methods: a) At the application layer, using Transport Layer Security (TLS); b) At the network layer, using Internet Protocol Security (IPSec); c) Secure Shell (SSH) [for remote administration of systems *only;* no protectively marked data is permitted to transfer via SSH]; d) A bespoke solution assured by the Department's risk management process and approved by Design Authority (such as the departmentally approved encryption solutions).
10.6.3	The protocols, protocol suites and techniques described in Clause 10.6.2 MUST be deployed and configured in accordance with Design Authority approval and other relevant security standards (e.g. SS-029 Security Standard – Securely Serving Web Content for HTTPS applications).
10.6.4	Encrypted sessions MUST re-negotiate new symmetric keys after one of the following criteria is met: a) The "counter" in CTR or GCM mode has exhausted all possible unique values for the initialisation vector. The standard deployment using AES permits 64GB of information to be passed and no more; b) 8 hours have passed, which is a best-practice requirement to prevent initialisation vector re-use where the exact amount of data transmitted cannot be tracked and/or different modes are used.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7.7 Encryption at Rest

Reference	Security Control Requirement
10.7.1	All user-writable partitions on portable devices (laptops, phones, etc.) and portable storage media MUST be encrypted at the media-level (i.e. Full Disk Encryption (FDE)).
10.7.2	Information held encrypted at rest MUST also be integrity protected.
10.7.3	Where multiple layers of encryption are available (e.g. media-level and database field-level), each layer MUST be applied proportionally to mitigate risks identified during the risk assessment process.
10.7.4	The encryption software deployed on devices as described in Clause 10.7.1 MUST require sufficient entropy as part of the authentication mechanism. In a scheme that uses a password as the authentication mechanism, this equates to a password that is of sufficient length and complexity to match the requirements in the password policy defined for the system.
10.7.5	The encryption software deployed on devices as described in Clause 10.7.1 MUST restrict the number of authentication attempts within any given time interval. Where the number of attempts and time interval are not specified as part of the product's certification, these values MUST be restricted to a value defined in the password policy for the system in question.

7.8 Passwords

Reference	Security Control Requirement
10.8.1	Authentication information which grants authorised access to asset(s) MUST: a) Not be stored in plain text or in any reversible format; b) Be *salted* with at least 64 bits of *pseudorandom data*; c) Be *hashed* using a method described in the latest approved version of DWP Approved Cryptographic Algorithms.

7.9 Cryptographic Key Management

Reference	Security Control Requirement
10.9.1	Cryptographic keys MUST be managed and protected in accordance with the controls present in SS-002 Security Standard – Public Key infrastructure.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

10. Document Reference

Document Name	Location	Version
Design Authority Exceptions Process		
DWP Patching Policy		
DWP Password Policy		
DWP Approved		

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Document Name	Location	Version
Cryptographic Algorithms		
FIPS PUB 140-2 – Security Requirements for Cryptographic Modules	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS PUB 186-4 – Digital Signature Standard (DSS)	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf	July 2013
PKCS#11 Cryptographic Token Interface Base Specification	http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.pdf	Version 2.40, April 2015
RFC 5280 Section 4, Certificate and Certificate Extensions Profile	https://tools.ietf.org/html/rfc5280#section-4	May 2008
FIPS PUB 197 – Advanced Encryption Standard (AES)	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf	November 2001
OWASP Application Security Verification Standard	https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf	Version 3.0, October 2015
HMG IA Standard No. 4 – Protective Security Controls for the Handling and Management of Cryptographic Items (OFFICIAL-SENSITIVE)	# Obtainable from the National Cyber Security Centre (NCSC) by request only #	Issue 7.0, July 2015
PKCS #1 v2.2: RSA Cryptography Standard, Section 7.1 – RSAES-OAEP	https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf	Version 2.2, October 2012
DWP Approved Encryption Solutions		

11. Definition of Terms

Terms	Definition
Cryptographic Algorithm	A well-defined computational procedure that takes variable input(s) and produces an output used in the preservation of confidentiality, integrity, authenticity or accountability.
Cryptographic Hardware	Any hardware that is used in the protection or creation of cryptographic material (e.g. Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs)).
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, non-repudiation and accountability; including, but not limited to: devices, products, systems, key variables and code systems.
Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Terms	Definition
	an entity with knowledge of the key can reproduce, reverse or verify the operation, while an entity without knowledge of the key cannot.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).
Cryptographic Software	Software used to protect the confidentiality, integrity, authenticity or accountability of information systems, or software used to generate cryptographic key material to be used for the above.
Digital Signature	The result of a cryptographic transformation of data that, when properly implemented with a supporting infrastructure and policy, provides the services of: 1. Origin authentication; 2. Data integrity authentication; 3. Signer non-repudiation.
Encrypt-then-MAC	The plaintext is first encrypted, and then a Message Authentication Code (MAC) is produced based on the resulting ciphertext. Antonymous to MAC-then-encrypt and encrypt-and-MAC.
Ephemeral Key	A key generated at each individual execution of a key exchange process. The opposite of a static or persistent key.
FIPS 140-2	A cryptographic standard created by the American National Institute of Standards and Technology (NIST) used to certify cryptographic modules against four increasing security levels. Where later versions of FIPS 140 are approved for use by NIST, e.g. FIPS 140-3, we will also accept these certifications as equivalent.
Hash (also known as: Cryptographic Hash, Message Digest, Digest)	The result of a cryptographic hash function, an algorithm with the following properties: 1. Variable size input; 2. Fixed size output; 3. Efficient; 4. Pre-image resistance (the function is computationally difficult to reverse); 5. Second pre-image resistance (Given a message, it is computationally difficult to find a message with the same cryptographic hash); 6. Collision resistance (it is computationally difficult to find any two messages with the same cryptographic hash).
Initialisation Vector (IV)	An input to some cryptographic functions, usually used to remove deterministic properties of ciphertext. IVs may

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Terms	Definition
	have a requirement to be either: 1. Unique; 2. Random Or both, depending on the cryptosystem.
Mode of Operation	A process that describes how to repeatedly apply a single-block operation so that it can be used to encrypt or decrypt data larger than the block size.
Pseudorandom Data	Data that satisfies statistical tests for randomness but is produced by a reproducible mathematical process (i.e. an algorithm).
Salt	Random data used as an additional input to a cryptographic hash function, mitigating password-related attacks such as dictionary attacks and pre-computed rainbow table attacks.
Secret Parameters	Any parameter passed to a cryptographic algorithm which would cause damage to confidentiality, integrity, authenticity or accountability if it was disclosed to an unauthorised party.

12. Glossary

Abbreviation	Definition
AES	Advanced Encryption Standard – defined in FIPS 197. Different *modes of operation* are covered in different documents
ANSI	American National Standards Institute
API	Application Programming Interface
CTR	Counter – a mode of operation for a symmetric block cipher
DA	Design Authority
DSA	Digital Signature Algorithm – defined in FIPS 186-4. Also known as the Digital Signature Standard (DSS).
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm – defined in FIPS 186-4.
FIPS	Federal Information Processing Standard
FIPS 140-2	The NIST standard used to certify cryptographic modules at four differing levels of security
GB	Gigabyte
GCM	Galois-Counter Mode – a mode of operation for a symmetric block cipher
GCSP	Government Security Classification Policy
GSI	Government Secure Intranet
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IPSec	Internet Protocol Security

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Abbreviation	Definition
ISO	International Organisation for Standardisation
IV	Initialisation Vector
KDF	Key Derivation Function
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OAEP	Optimal Asymmetric Encryption Padding
OWASP	Open Web Application Security Project
PBKDF	Password-Based Key Derivation Function
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standard
PRF	Pseudorandom Function
RSA	Rivest, Shamir and Adleman's asymmetric encryption algorithm
SEM	Secure Email
SHA	Secure Hashing Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
TPM	Trusted Platform Module
VM	Virtual Machine
X.509	The standard format for digital certificates. Defined in RFC 5280 Section 4

13. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27002:2013, NIST 800-53, and the OWASP Application Security Verification Standard (ASVS).

SS-007 Security Standard – Use of Cryptography	DWP Controls Catalogue - Baseline Control Set	
Control Statement	**Control Reference**	**Descriptor**
10.1.1	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.1.2	AP01	Procedures shall be implemented to control the installation of software on operational systems.
10.1.3	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces,

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-007 Security Standard – Use of Cryptography	DWP Controls Catalogue - Baseline Control Set	
		over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.1.4	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.1.5	AP01	Procedures shall be implemented to control the installation of software on operational systems.
10.2.1	CY09	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.2.2	CY09	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.2.3	CY09	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.2.4	CY09	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.2.5	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.2.6	CY08	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.
10.2.7	CY06	Policies and procedures shall be established, and supporting business processes and technical measures

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-007 Security Standard – Use of Cryptography	DWP Controls Catalogue - Baseline Control Set	
		implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.3.1	CY07	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.
10.3.2	CY07	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.
10.4.1	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.5.1	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.6.1	MW01	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.
10.6.2	CY09	The provider shall use secure (e.g., non-clear text and

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-007 Security Standard – Use of Cryptography	DWP Controls Catalogue - Baseline Control Set	
		authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.6.3	CY09	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.6.4	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.7.1	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.7.2	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.7.3	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.7.4	AC19	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
10.7.5	AC19	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
10.8.1	CY06	Policies and procedures shall be established, and supporting business processes and technical measures

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-007 Security Standard – Use of Cryptography	DWP Controls Catalogue - Baseline Control Set	
		implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.9.1	CY01, CY04, CY05, CY06, CY07, CY08, CY09, CY10	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.