OFFICIAL

highways england

INFORMATION SECURITY

Data Security Standard

Document Purpose
This document describes how Highways England data shall be secured.

cybersecurity@highwaysengland.co.uk

1 Document Control

Document Title	Data Security Standard
Author	Jenny White
Owner	Information Security
Distribution	Highways England
Document Status	Under Review

1.1 Revision History

Version	Date	Description	Author
V1.0	26/03/19	First Version	Scott Bartlett

1.2 Reviewer List

Name	Role
Jenny White	Information Security lead
Scott Bartlett	Information Security lead Analyst
Davin Crowley-Sweet	Chief Data Officer

1.3 Approvals

Name	Signature	Title	Date of Issue	Version
Tony Malone		Chief Information Officer		1.0

This document is copyright to Highways England.

2 Contents

1 Document Control 2
2 Contents 3
3 Definitions 3
4 Overview 4
5 How should this document be used? 4
6 Information Security Map 4
7 Information Access 5
8 Information in Transit 6
9 Information at Rest 9
10 Cryptographic Deployments 10
11 Information Destruction 13
12 Contact Us 13

3 Definitions

Solution – A collection of information systems that together comprise a capability or service being delivered to Highways England.

Information System –An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. Within Highways England, this includes both hardware and software components

Information Assets – An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.

Information Asset Owner – Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, added and removed, how it is moved, and who has access and why. As a result, they are able to understand and address risks to the information, and ensure that it is correctly used. They provide a written judgement of the security and use of their asset annually to support the audit process.

This document is copyright to Highways England.

4 Overview

This document details the logical and administrative standards required to provide appropriate protection to Highways England data. This protection is in line with the Highways England threat landscape, and is in accordance with the Information Security Data Handling requirements.

5 How should this document be used?

This document shall be used by project sponsors, service delivery managers and relevant suppliers to enable solutions to be designed, procured and configured to meet the baseline standard of security defined in Information Security Data Handling requirements.

6 Information Security Map

The following figure illustrates where this document sits in the wider Information Security document set.

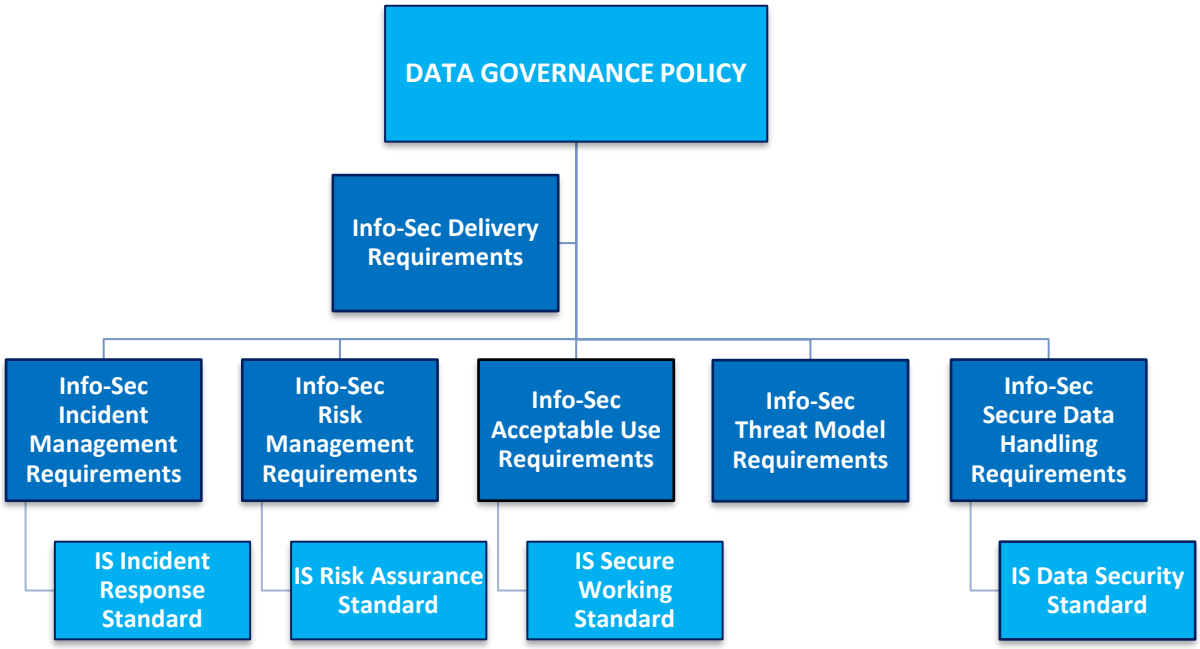

Figure 1 – Information Security Document Set

This document is copyright to Highways England.

7 Information Access

This section specifies who can be given access to different data types and what employment screening checks should be performed.

7.1 OFFICIAL

All users requiring access to OFFICIAL information (including OFFICIAL SENSITIVE) shall have undergone the Baseline Personnel Security Standard (BPSS) checks which consist of;

- Confirmation of right to work in the UK.
- Identification checks.
- Criminal record checks.
- Employment history for the last 3 years.

7.2 OFFICIAL-SENSITIVE

All users requiring access to OFFICIAL-SENSITIVE information shall in addition to the BPSS have a business need for accessing that information which must be confirmed by either the information originator or relevant information asset owner (IAO).

Certain roles in Highways England may require the Security Clearance (SC) level of government security vetting. A BPSS is required as a pre-requisite for applying for SC.

This document is copyright to Highways England.

8 Information in Transit

This section details the geographical, physical and logical restrictions to the transfer of information from one information system to another. Where exceptions are required, Highways England Information Security team must be consulted in advance so that the Information Security risk can be fully understood by them and those requesting it.

8.1 Geographical Standards

This section defines the geographical boundaries through which information shall transit through.

8.1.1 OFFICIAL-SENSITIVE

No data marked OFFICIAL-SENSITIVE shall transit outside of the European Economic Area (EEA). The countries that comprise the EEA are detailed at https://www.gov.uk/eu-eea.

8.1.2 OFFICIAL

OFFICIAL data that is not marked OFFICIAL SENSITIVE may transit outside of the EEA only as part of a recognised solution that has been through the Highways England Information Security Assurance process.

8.2 Physical Standards

This section defines the physical standards by which information may be transferred.

8.2.1 OFFICIAL-SENSITIVE

Any physical device or medium that is transmitting data with the OFFICIAL-SENSITIVE handling caveat both tagged and untagged shall support and implement the OFFICIAL-SENSITIVE logical standards of protection defined in section 8.

8.2.2 OFFICIAL

Any physical device or medium that is transmitting OFFICIAL data both tagged and untagged shall support and implement the OFFICIAL logical standard of protection defined in section 8.

8.3 Logical Standards

This section details the logical standards of transport layer protection to be applied to data during transit. Where message based protections are applied the standards referenced in section 9.3 shall be followed. Any cryptographic functions shall be implemented in accordance with section 10.

8.3.1 OFFICIAL including OFFICIAL-SENSITIVE

OFFICIAL data, including that marked OFFICIAL-SENSITIVE, shall be protected in transit by the following cipher suites.

This document is copyright to Highways England.

8.3.1.1 Transport Layer Security (TLS) Based Cipher Suites

Data shall be protected using Combination 1 of the suite B profile for TLS, defined in RFC6460 and detailed by the National Cyber Security Centre (NCSC). For completeness this is detailed in table 2 below.

Protocol	TLS 1.2
Symmetric Cipher	AES with 128-bit key in GCM mode
Pseudo-random function	TLS PRF (with SHA-256)
Authentication	ECDSA-256 with SHA-256 on P-256 curve
Key exchange	ECDH using P-256 curve

Table 2 - NCSC Combination 1 of the Suite B profile for TLS (RFC6460)

8.3.1.2 IPSec Based Cipher Suites

Data shall be protected using the NCSC foundation profile for IPSec. For completeness this is detailed below in table 3.

IKEv1	**Selection**
Symmetric Cipher	AES with 128-bit keys in CBC mode (RFC3602)
Pseudo-random function	HMAC-SHA-256 (RFC4868)
Diffe-Hellman Group	Group 14 (2048-bit MODP Group) (RFC3526)
Authentication	X.509 certificates with RSA signatures (2048 bits) and SHA-256 (RFC4945 and RFC4055)
ESP	
Symmetric Cipher	AES with 128-bit keys in CBC mode (RFC3602)
Integrity	SHA-256 (RFC4868)

Table 3 – NCSC Foundation Profile for IPSec

8.3.1.3 Secure Shell (SSH)

Any use of SSH shall be in accordance with RFC 4251 and RFC 8270 and shall only utilise public/private key pairs to authenticate user sessions. SSH protocol version 2 or greater shall be used and shall be configured to disallow the following insecure ciphers (table 4) and hashing algorithms (table 5):

OpenSSH Option	Permissible Cipher Options	Notes
Cipher	• aes256-ctr • aes192-ctr • aes128-ctr • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly1305@openssh.com • aes128-cbc • aes192-cbc • aes256-cbc	These are the cipher directives supported by OpenSSH. Alternative SSHD implementations might use a different formulation to describe these ciphers.

Table 4 – Permissible Ciphers for SSH

This document is copyright to Highways England.

Open SSH Option	Permissible Hashing Algorithms	Notes
MACs	• hmac-sha2-256 • hmac-sha2-512	These are the hashing algorithms supported by OpenSSH. Alternative SSHD implementations might use a different formulation to describe algorithms.

Table 2 – Insecure Hashing Algorithms for SSH

For services intended to be deployed at an outstation, in-station or RCC further implementation standards defined in MCE 1126 shall be followed.

8.3.1.4 Remote Desktop Protocol

Any use of remote desktop protocol shall not utilise pre-shared keys or passwords for authentication and encryption. Instead TLS or IPSec should be used in accordance with the standards defined at 8.3.1.1 and 8.3.1.2. In addition, any RDP service shall be configured to:

- Support only Version 6 or greater of the RDP protocol.
- Support only Connections that feature network level authentication.
- Utilise wherever possible jump servers.
- Randomise listening ports.
- Limit access based on genuine need.
- Lockout accounts after successive failed login attempts.

8.3.1.5 Public Key Infrastructure Deployment

All PKI deployments shall be done in accordance with NCSC guidance titled Provisioning and Securing Security Certificates.

This document is copyright to Highways England.

9 Information at Rest

This section details the standards required to physically and logically secure data at rest.

9.1 Geographical Standards

This section defines the geographical boundaries in which information types shall be stored.

9.1.1 OFFICIAL-SENSITIVE

Data marked OFFICIAL-SENSITIVE may not be stored outside of the European Economic area (EEA). The countries that comprise the EEA are detailed at https://www.gov.uk/eu-eea.

9.1.2 OFFICIAL

Data that is not marked OFFICIAL-SENSITIVE may only be stored outside the EEA with the agreement of the Data and Information Governance team comprising of the Cyber Security, Information Protection, and Records Management teams.

9.2 Physical Standards

This section defines the physical standards around the storage of information.

9.2.1 OFFICIAL including OFFICIAL-SENSITIVE

All information storage locations shall meet our server room standards. Where appropriate a gap analysis of the locations shall be conducted by project sponsors or service delivery managers using the NCSC cloud security principles and provided to Highways England Information Security.

9.3 Logical Standards

This section details the logical standards of protection to be applied to data at rest. Any cryptographic functions shall be implemented in accordance with section 10.

9.3.1 OFFICIAL including OFFICIAL-SENSITIVE

All OFFICIAL information including OFFICIAL-SENSITIVE shall be stored at rest using the Advanced Encryption Standard (AES) symmetric block cipher with either a 128, 192 or 256-bit key size.

This document is copyright to Highways England.

10 Cryptographic Deployments

Where cryptographic functions are in use the solution shall ensure the following:

10.1 Cryptographic Responsibility

All solutions that utilise elements of cryptography shall have a custodian that is responsible for the management and accounting of all cryptographic elements for that specific system.

The custodian shall nominate a deputy to take responsibility in the event of absence to ensure a continuous service.

The custodian and nominated deputy shall be appropriately cleared and recorded within the systems information security assurance documentation. Highways England Information Security will provide clearance requirements on request.

Any individual who handles cryptographic elements of a system shall gain the approval of the custodian and shall be appropriately cleared and trained to use such elements. This includes individuals involved in the transportation of keys, as well as users. For example, the custodian may be the project sponsor or the information asset owner for a system.

10.2 Cryptographic Assurance

All systems that use cryptographic elements shall undergo the Highways England Information Security Risk Assurance process to ensure:

- The level of cryptography is appropriate for the level of risk the solution attracts.
- A documented design of the cryptographic elements exists.

10.3 Removable media

Removable media shall only be configured and deployed to support cryptographic functions permitted by this standard.

Any use of removable media to shall be in accordance with the Highways England Secure Data Handling Requirements.

All removable media in use shall be for accounted for by the custodian at all times.

10.4 Key Generation

Only the custodian is permitted to request key pair generation. The method of key generation shall be documented in the assurance documentation for the system.

All requests to generate new keys shall be validated by separate forms of communication from the custodian. For example, an email and a phone call will be required.

All keys shall have a random generation process such that one key cannot be obtained

This document is copyright to Highways England.

from another. This generation process should be an RFC compliant implementation of a cipher or algorithm approved by this standard.

10.5 Key Distribution

Private keys and pre-shared keys (PSK) shall be distributed securely so that only authorised individuals can access the keys.

The distribution process shall be fully documented within the system accreditation documentation.

The distribution process shall incorporate a method to confirm receipt of the keys.

The distribution of all keys shall be secure to prevent the theft of keys in transit.

All key distribution events shall be logged to an individual user so that the process can be audited at a later date.

10.6 Key Storage

All keys shall be protected from unauthorised access.

All keys shall be stored away from encrypted data.

All Root Certificate Authority keys shall be kept in a dedicated safe.

All processes and procedures involving key storage shall be documented in the solution accreditation documentation.

All keys shall be appropriately and clearly labelled to ensure they are easily identified in case of an incident or destruction.

10.7 Key Updates

All keys shall have a defined key lifecycle. Keys used for encryption shall be changed periodically as indicated in the system accreditation documentation or in the event of a breach.

A defined change process for keys shall be fully documented within the accreditation documentation for the system.

10.8 Key Revocation

Revocation of keys and digital certificates due to a suspected compromise shall be authorised by the custodian and reported to Highways England Information Security.

Any use of certificate revocation lists either manual or automated shall ensure compromised or stale certificates are revoked within 1 hour of discovery.

10.9 Key Compromise

Any key compromise shall be classed as an Information Security Incident and shall follow the Highways England Incident Response standard or solution specific

This document is copyright to Highways England.

incident response plan. This response plan shall be detailed within the information security assurance documentation.

10.10 Key Backup

Keys shall be backed up or archived appropriately as defined by the business continuity plan for the solution.

10.11 Key Destruction

Assurance documentation shall include a process of data destruction that includes cryptographic keying material. Where the destruction process has not been documented, Highways England Information Security shall be consulted prior to the destruction of cryptographic elements by the custodian.

10.12 Logging and auditing of key management related activities

All key related activities shall be logged either automatically or manually.

All logs recorded shall be specific to individual users.

The custodian shall review logs regularly to ensure that unauthorised users have not accessed cryptographic elements.

10.13 Content inspection

Where encryption is to be used, the content of the data shall be inspected at source or destination unless traffic is routed through the Highways England proxy solution.

This document is copyright to Highways England.

11 Information Destruction

This section details the technical requirements to ensure secure destruction of information using commercial best practice.

11.1 OFFICIAL-SENSITIVE

11.1.1 Hardcopy (paper)

Loose-leaf hardcopy information marked OFFICIAL SENSITIVE should be disposed of in the secure disposal box placed in each Highways England office. Where this is not available, it must be shredded in a cross cut shredder with no greater than 4mm shred size.

Registered files marked OFFICIAL SENSITIVE shall be disposed of by the Records Management Team according to their procedure.

11.1.2 Optical and Floppy

Optical media (CDs, DVDs, BDs etc) and any legacy floppy discs marked OFFICIAL SENSITIVE must be shredded in a cross-cut shredder with no greater than 4mm shred size.

11.1.3 All other media

Re-useable Media such as USB memory sticks, portable hard drives and non-portable hard drives shall be assumed to carry or have carried OFFICIAL-SENSITIVE information.

Re-usable media that is being decommissioned and not used by Highways England again shall undergo appropriate physical destruction by a commercial company by shredding and shall provide Highways England with a certificate of destruction. if it is to be decommissioned and not reused. The company shall also allow the destruction to be witnessed by a Highways England delegate who shall also confirm to Highways England Information Security that the destruction took place.

Reusable media for re-use within Highways England shall be over-written to the DoD 5220.22-M standard.

11.2 OFFICIAL

As OFFICIAL-SENSITIVE less the Highways England witnessing and declaration of destruction.

---

12 Contact Us

For errors, omissions and general queries email:

cybersecurity@highwaysengland.co.uk

This document is copyright to Highways England.