highways england

INFORMATION SECURITY

SECURE DATA HANDLING REQUIREMENTS

Document Purpose

This document describes how Highways England data must be handled in the context of information security.

informationsecurity@highwaysengland.co.uk

1 Document Control

Document Title	Secure Data Handling Requirements
Author	Jenny White
Owner	Information Security
Distribution	Highways England
Document Status	Awaiting Approval

1.1 Revision History

Version	Date	Description	Author
1.3	26/06/15	Annual review	Harry Payne
1.4	11/02/16	Annual review	Harry Payne
1.5	24/03/17	Annual review	Harry Payne
1.6	04/07/17	Annual review	Harry Payne
1.7	15/01/18	Annual review	Liam Feeney, Eamonn Patton, Harry Payne
1.8	24/01/19	CDO Task Revision	Simon Andrews
1.9	03/02/19	Addition of sections	Scott Bartlett
2.0	14/03/19	Re-draft	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		2.00

2 Overview

The information produced and processed by Highways England is a valuable business asset. It is therefore essential that all information for which it has responsibility is used, communicated, transferred, stored, and disposed of in a manner that complies with legal and regulatory requirements, and with the broader information management framework in place at Highways England. Highways England is committed to properly protecting the information that it holds. These requirements have been agreed by the Highways England Leadership Team.

Appropriate handling and storage of company information is the responsibility of every user of Highways England's data. The technical processes in use to facilitate this are ineffective unless the correct procedures are carried out in a careful and consistent manner.

3 Who Should Use This Document

This document communicates security requirements to all users of Highways England data across its entire lifecycle covering its use, communication, transfer, storage, and disposal.

4 Information Security Map

Figure 1 shows where this document sits in the wider information security system.

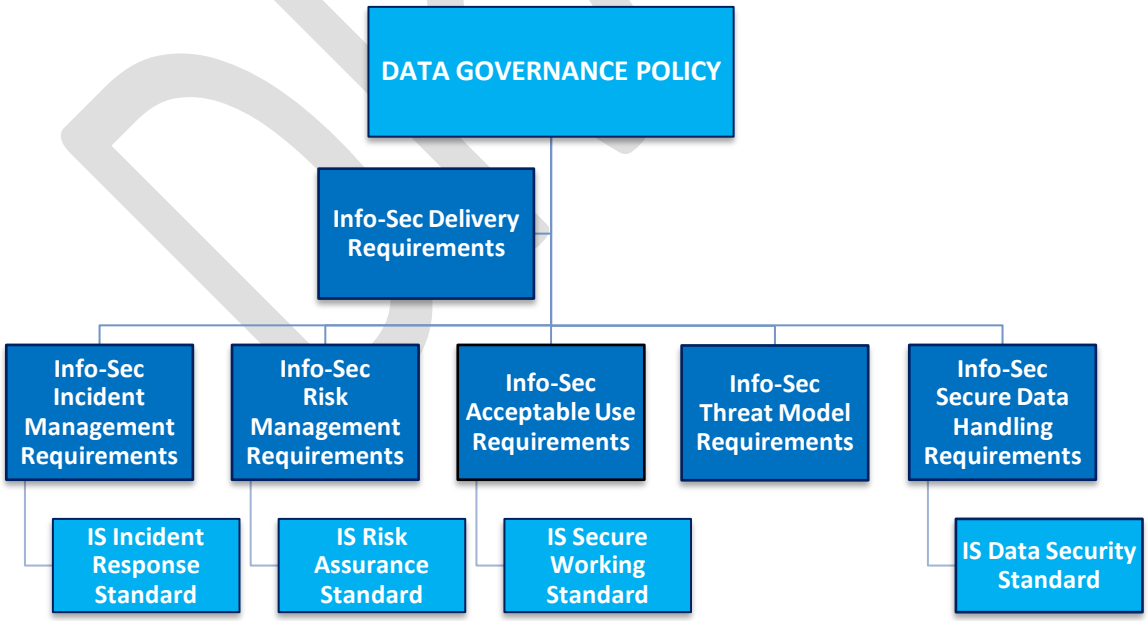

Figure 1 – Information Security System

5 Contents

6 Definitions

Users – The term used to mean persons who fall within the scope of these requirements.

Offshoring – The term used to describe the persistent storage of information outside of the United Kingdom's geographical boundary.

7 Scope

These requirements shall apply to all information obtained and processed by Highways England and its users and suppliers. It therefore relates to all information systems, digital and non-digital, and will cover all information within Highways England that may be:

- Digitally stored on fixed computers
- Transmitted across networks
- Printed out or written on paper
- Sent internally or externally by post, courier, or fax
- Stored on removable and other electronic media
- Spoken in face-to-face conversation or over the telephone.

8 Information Security Classifications

Information created and received by Highways England shall be classified according to the sensitivity of its contents. Classification and controls must take account of organisational needs for sharing or restricting information, and the associated impacts and risks, e.g. unauthorised access or damage to the information.

8.1 OFFICIAL

8.1.1 Description

The classification used within Highways England for all information is OFFICIAL. Information classified as OFFICIAL includes but is not limited to:

- Routine correspondence (where there is no confidentiality requirement)
- One-off exchanges with third parties
- Employee newsletters
- Internal phone directories
- Inter-office memoranda
- Internal policies and procedures
- Questions around project delivery

8.1.2 Impact of Compromise

Compromise of OFFICIAL information is likely to affect individual departments within Highways England and may cause local media coverage or give external attackers knowledge which could indirectly lead to a further compromise of Highways England data.

8.1.3 Marking

There is no requirement to explicitly mark OFFICIAL information.

8.2 OFFICIAL SENSITIVE

8.2.1 Description

There is a subset of information produced/processed by Highways England where a compromise of the information confidentiality, integrity or availability could have more damaging consequences for Highways England, its staff or its business partners. This information, must be caveated OFFICIAL-SENSITIVE. Such information includes but is not limited to:

- Information that could be used to compromise the security of Highways England information systems as internal IP addresses, details of security measures and versions of security products.
- Risk Registers for Operational level risks and above.
- Personal Identifiable information. (Can be appended with the PERSONAL tag)
- Financial and commercially sensitive information. (Can be appended with the COMMERICIAL tag)

The OFFICIAL-SENSITIVE caveat is not a separate classification; it is tool to denote OFFICIAL information that is of a particular sensitivity. Further clarification and

details of the government classification scheme upon which Highways scheme is based can be found here.

8.2.2 Impact of Compromise

Compromise of OFFICIAL-SENSITIVE information will likely result in significant adverse impact, embarrassment or penalties to Highways England, its stakeholders, employees, or members of the public.

8.2.3 Marking

Both physical and digital types of OFFICIAL-SENSITIVE information should be conspicuously marked as such.

8.3 Other

If any information is held that is perceived to be above these classifications, then guidelines for handling such data must be sought from Highways England Information Security team within 48 hours of discovery.

9 Information Access

Internal and external access to Highways England data is governed by the security classification of the information which itself is derived from the government classification scheme. Which as a whole is also subject to the freedom of information act.

9.1 OFFICIAL

For information classified as OFFICIAL all persons requiring access, both physical and logical must undergo appropriate employment screening checks defined in the Baseline Personal Security Standard (BPSS).

9.2 OFFICIAL-SENSITIVE

For OFFICIAL-SENSITIVE information all persons who require access must have a stated business need to access the information in addition to the requirements of OFFICIAL. The information in question must only be used in line with this business need and access revoked once the business need is no longer valid.

9.3 Information Aggregation

Where persons are given privilege levels that provide access to aggregated OFFICIAL and OFFICIAL-SENSITIVE information and associated accounts then individuals must undergo and attain the Security Check (SC) level of vetting. This is further defined within the Information Security Data Security Standard.

10 Information Transfer

10.1 Methods of Transfer

Information can be transferred in a variety of ways, both direct and indirect. These include:

- Spoken Word
- Post, fax, or e-mail
- Internet or intranet
- Portable Media (including CDs, DVDs, Memory Sticks and Data Cartridges)
- Electronic File Transfer
- Web Portals
- Print, Film, Fiche, Video, DVD Images

10.2 OFFICIAL

Highways England Information must only be transferred to persons who are authorised to have access to it. There must be adequate security measures in place at the virtual and/or physical destination. The definition of adequate is defined in the IS Data Security Standard, where a security measures adequacy is unclear guidance shall be sought from the Highways England Information Security team.

10.3 OFFICIAL-SENSITIVE

Where OFFICIAL-SENSITIVE information is being transferred, Information Asset Owners will typically require additional assurance around the security measures in place. OFFICIAL-SENSITIVE information must not be sent or physically taken off-site without the appropriate authorisation by the Information Asset Owner or someone who the Information Security team recognise as a suitably delegated authority.

10.4 Geographical Restrictions

In all cases the route through which information travels both physically and logically shall be in accordance with the boundaries defined in the IS Data Security Standard.

11 Information Storage

Information shall be stored throughout its existence in an environment suited to its format and security classification, to ensure its preservation from physical harm or degradation and its security from loss or unauthorised access. Technical requirements are detailed in the IS Data Security Standard

11.1 Physical Protection

Information in all formats should be stored in conditions that protect it from threats to its physical integrity through unnecessary wear and tear; specific threats such as fire, flooding, and magnetic fields; and environmental extremes or fluctuations. Where the information system or its data is classed as business-critical special storage equipment and environments should be used.

Physical access to information should be restricted by locking it in rooms, cabinets, drawers, and other storage areas or units when not in use, and by ensuring that files and computer monitors are not left open to general or casual view.

11.2 Logical Protection

Protection from unauthorised access may require mechanisms such as password-protection or encryption of digital files and data, and sign-in sheets or request dockets for access to non-digital information. Further information about what is required detailed in the IS Authenticator Standard and IS Data Security Standard.

Where information is stored on a mobile device (e.g. PDA, USB drive, laptop), special care must be taken to ensure that the device is physically protected from theft, loss, or damage, particularly if it is transferred or used away from Highways England business sites. Further information is detailed in the IS Remote Working Standard.

11.3 Storage Location

Information, whether original or duplicate, shall never be kept outside Highway England owned systems (e.g. on PC hard drives, on CDs or other removable media) except as part of a solution that Highways England has formally procured from a supplier or as a temporary off-line copy driven by an immediate business need to work off-site or off-line, or for authorised transfer to other users or systems.

11.3.1 Offshoring

Information shall only be kept in the geographical boundaries defined in the IS Data Security Standard. Any exception to these boundaries shall require prior agreement from Highways England Information Security.

11.4 Information Availability

Information should be stored in systems and according to classifications, frameworks and procedures that enable it to be readily identified and retrieved throughout its existence.

Information held in digital formats should be managed and stored in such a way as to ensure usability and accessibility through time.

12 Information Destruction

Information should only be destroyed in the ordinary course of business; information subject to open or pending investigation, audit, or litigation and that is required for legal retention purposes must not be destroyed.

12.1 Personal Identifiable Data

The Highways England Information Rights team must always approve destruction relating to personal identifiable data in cases where Highways England are the data controllers.

12.2 Physical Destruction

12.2.1 OFFICIAL

Physical destruction of digital and non-digital media shall be carried out to standards appropriate to the security classification.

12.2.2 OFFICIAL-SENSITIVE

Information must be destroyed securely, and the act of destruction should be certified or signed off.

12.3 Logical Destruction

Where electronic data is to be erased but the medium left intact, it must be deleted to the extent appropriate to the security classification, e.g. by over-writing files or reformatting disks.

12.4 Destruction Standards

The technical destruction standards appropriate to each security classification, for information held in digital or non-digital formats shall be done in accordance with the IS Data Security Standard.

13 Contact Us

For errors, omissions and general queries email:

cybersecurity@highwaysengland.co.uk