File Reference: **HCSL 4/14/019**

****

Title of Document: **Statement of Highways England IT Security Policy**

****

This document has been examined and has been approved for issue.

Highways England
IT Security Policy

Amendment History: This document was reviewed in July 2015

Amendment Version: 3.4

Approved: Victoria Williams
Highways England IT Security Officer

Date: July 2015

Distribution: All Highways England staff

Table of Contents

1. INTRODUCTION AND SCOPE 3
2. ORGANISATION 5
3. RESPONSIBILITIES 6
4. ASSET CONTROL 9
5. RISK ASSESSMENT AND RISK MANAGEMENT 10
6. RISK MANAGEMENT ACCREDITATION DOCUMENT SETS 11
7. CONTINGENCY PLANNING 12
8. LEGAL REQUIREMENTS 13
9. AUDIT AND COMPLIANCE MONITORING 14
10. EDUCATION AND AWARENESS 15
11. INCIDENT HANDLING 16
12. THE GOVERNMENT SECURITY CLASSIFICATION POLICY 17
13. LEVELS OF PROTECTION AND SECURITY CLASSIFICATION 18
14. RECORDS POLICY: PAPER AND ELECTRONIC RECORDS 20

ANNEX A: GLOSSARY 21
ANNEX B: CONTACTS AND FURTHER GUIDANCE 22

1. INTRODUCTION AND SCOPE

1.1. This document is a statement that sets out the policy for the security requirements covering the Information systems within Highways England. The policy is designed to protect the confidentiality, integrity and availability of information handled on Highways England IT systems. It is produced in accordance with Her Majesty's Government (HMG) IT Security Policy and forms part of the Highways England Information Security Policy.

1.2. The policy covers all Highways England computer systems including the hardware, the software and all information held or processed on them. This policy is applicable to all Highways England, and to companies and individuals contracted to provide or to maintain IT systems and services.

1.3. IT is an essential tool for the delivery of Highways England business objectives and the protection of this investment by way of appropriate security measures is vital. These encompass physical, personnel, and technical security measures.

1.4. Highways England is required to comply with the Government Security Framework and aligns itself with the ISO 270001 Information Management standard. The Company is therefore required to:-

1.4.1. Establish and enforce an IT Security Policy consistent with HMG's IT Security Policy as reflected in the Security Policy Framework (SPF);

1.4.2. Maintain an organisation to direct and manage information security;

1.4.3. Ensure that risks are reduced to an acceptable level by applying protective measures which are based on risk assessment and the classification of information, and which conform to appropriate minimum standards;

1.4.4. Limit access to information and other IT assets to those whose duties require it and who have the necessary authority and security clearance;

1.4.5. Ensure that personnel are aware of the IT Security Policy and practice to the extent that their duties require, and fully understand their responsibilities (including their legal obligations); and

1.4.6. Monitor and review HMG information security arrangements to ensure that policy, standards, and procedures remain relevant and effective.

1.5. The aim of the IT Security Policy is to ensure that all IT systems throughout the Company and all information held on those systems are appropriately protected so as to maintain:-

1.5.1. **Confidentiality** of data to prevent unauthorised access and disclosure;

1.5.2. **Integrity** of data to prevent accidental or unauthorised alteration or deletion of data; and

1.5.3. **Availability** and reliability of IT systems and data to the business needs.

1.6. Protection should be proportionate to the value of the asset, cost-effective and relate to the risks. Security practice and processes should have a limited impact on users and reflect the priorities of our business.

1.7. This document will provide a high-level statement of the framework within which security policy will operate.

1.8. Detailed IT security standards adopted by Highways England can be found in - IT Security Standards for PC Users.

1.9. Additional guidance is available in:

- The IT Security Guide
- Working Securely Away from the Office Guide
- Acceptable Use of ICT Equipment,
- Email Guide
- Internet Guide.

These documents have been approved and endorsed by the Company's Senior Information Risk Officer (SIRO) and the Chief Executive.

2. ORGANISATION

2.1. Highways England is a Government Company owned by the Department for Transport. Highways England is responsible for its information management and security and is expected to follow HMG and industry best practice in protecting its assets.

2.2. Highways England is registered with the Information Commissioners Office (ICO) in its own right, and is governed through a licence agreement with the Department.

2.2.1. The Departmental Security Officer (DSO) is the overall authority for security within the Department. The Highways England DSO is the FBS Director.

2.2.2. The Departmental IT Security Officer co-ordinates IT security for the Department on behalf of the DSO.

2.3. Within Highways England the organisation of security is as follows:

2.3.1. The Chief Executive has overall responsibility for all matters relating to Highways England security.

2.3.2. The Senior Information Risk Officer (SIRO) is a member of the Highways England Board personally nominated by the Chief Executive to oversee and approve all policies and procedures for information handling in the Company.

2.3.3. The day-to-day function for security is discharged by the Highways England Security Officer in the Information Management Group, CIO Office, in the Finance and Business Services (FBS) Directorate.

2.3.4. The Highways England IT Security Officer (ITSO) sits within the Information Management Group, CIO Office in FBS and has specific responsibility for this function. The ITSO is supported by the IT Security Administrator and IT Security Assistant.

2.3.5. The Agency Records Officer sits within Information Management, CIO Office, in FBS is responsible for Document Management.

2.3.6. The Data Protection Officer sits within the Information Management Group, CIO Office; in FBS is responsible for Data Protection issues.

2.3.7. An organisation chart for the Security Team is held in SHARE.

3. RESPONSIBILITIES

3.1. The specific responsibilities for Information Security in Highways England are as follows:-

3.1.1. The Highways England Senior Information Risk Officer (SIRO).

The SIRO is an executive familiar with information risks and leads the Company's response. The SIRO is the focus for the management of information risk at Board level.

The SIRO:

- Leads and fosters a culture that values, protects and uses information for the public good
- Owns the overall information risk policy and risk assessment process, tests its outcome, and ensures it is used
- Advises the Accounting Officer on the information risk aspects of his/her statement on internal control

3.1.2. The Highways England Chief Information Officer (CIO)

The CIO is an executive responsible for IT Strategy, Policy and investment across the organisation, and supports the SIRO by ensuring delivery of:

- A culture that values, protects and uses information for the public good
- Owns the overall information risk policy and risk assessment process, tests its outcome, and ensures it is used

3.1.3. The Highways England IT Security Officer (ITSO).

The ITSO provides a central point of contact for the Company with specific responsibility for developing IT security policy, standards and procedures, and for ensuring that the appropriate levels of IT security are implemented and maintained throughout the Company.

The ITSO promotes IT security awareness and training, oversees IT security reviews and the enforcement of IT security standards. The ITSO ensures the Company contributes to HMG's Security Incident Reporting Scheme and provides reports on IT security matters to the Agency Management Board and the Departmental ITSO.

3.1.4. The IT Security Administrator (ITSA).

The ITSA supports the ITSO in carrying out the day-to-day responsibilities for IT security. The ITSA provides policy advice and guidance, organises new initiatives, acts as project manager for IT security projects and liaises with other government agencies.

3.1.5. Heads of Divisions, assisted by line managers, have a responsibility to ensure that staff under their control, including contractors, are aware of IT security policy and practice to the extent that their duties require, and fully understand their responsibilities including their legal obligations. They ensure that IT system owners are nominated for all IT systems under their control and that IT system owners have the necessary authority and resources to carry out their security responsibilities.

3.1.6. IT system owners ensure that their systems conform to the aims and objectives of the IT Security Policy. To that end they shall ensure not only that appropriate security measures are in force and are understood, but that appropriate IT security training is available to users.

3.1.7. IT system owners are obliged to ensure that every major new or replacement IT system has a written statement of security policy such as a Risk Management Accreditation Document Set (RM-ADS).

3.1.8. IT system owners employing private contractors are responsible for specifying and agreeing the levels of security to be provided in their IT systems, specifying how the contractor will use the system to provide assurance of adherence to Agency IT Security Policy and monitoring that the specified security is achieved.

3.1.9. Users of IT systems are required to comply with the IT Security Standards and the requirements outlined in the IT Security Guide. IT users should also be aware of and follow any specific security measures applicable to the individual IT systems they use.

3.1.10. All staff involved in the modification or development of IT systems are obliged to ensure that systems are developed in line with the IT Security Policy and conform to all relevant security requirements.

3.1.11. The Internal Audit Division provides independent assurance that IT security arrangements and procedures are adequate and functioning properly. They recommend improvements in the security arrangements to business owners where necessary.

3.1.12. The Highways England Records Officer formulates policy and provides advice on:

- records and document management issues throughout the Agency to meet statutory and departmental requirements;
- controlled documents and the management, ownership and authorship responsibilities associated with them, including version control and archiving within a secure environment, whether physical or ICT based (SHARE);
- Freedom of Information issues.

3.1.13. The Highways England Records Officer develops and manages a Company-wide records management programme designed to ensure that records practices are effectively managed to meet the Company's needs, in line with the Public Records Act and National Archives requirements.

3.1.14. The Data Protection Officer is responsible for the Highways England Data Protection Policy and all DPA issues across the Agency.

3.1.15. The Freedom of Information Officer is responsible for the Company's FOI and Open Data policy and all FOI issues across the Company.

3.1.16. The Company Information Asset Owners are responsible for information protection and management for all Company information assets.

4. ASSET CONTROL

4.1.1. IT System Managers must ensure that a record of all IT assets, including hardware and software, is available and kept up to date.

4.2. Procurement of all IT assets must be handled by the CIO Office as the initial point of contact with IT Suppliers.

4.3. Disposal of all IT assets, including hardware and software, must be handled by through the appropriate IT Supplier, with ultimate responsibility lying in the CIO Office. Particular care must be taken in the case of IT systems that have been used for processing or holding information marked OFFICIAL SENSITIVE and/or use HMG encryption. Guidance is available from IT Security. Disposal of system that have been used for processing or holding information marked SECRET or TOP SECRET must only be disposed of under the guidance of IT Security.

4.4. Re-allocation of IT assets to another user shall only be done with the prior approval of the IT System Managers in the CIO Office. Similarly, re-location of IT assets within an office or between offices requires the prior approval by the CIO Office.

5. RISK ASSESSMENT AND RISK MANAGEMENT

5.1. All IT system owners must ensure that a proper risk assessment has been carried out for the IT systems for which they have responsibility. This will determine the nature and level of protective measures to be applied, based on the confidentiality, integrity and availability requirements of the information asset.

5.2. The risk assessment should take account of the following factors:

5.2.1. The threat e.g. damage, theft or destruction of equipment; disclosure, modification or unavailability of data;

5.2.2. The vulnerabilities of the IT system e.g. location, communication links, personnel;

5.2.3. The value of the assets and the information e.g. the full replacement cost of the equipment, the sensitivity of the information and its importance to the business; and

5.2.4. The impact of an IT security violation e.g. damage to the Company's reputation, the effect on personal safety or privacy, possible legal action, breaches of commercial confidence, financial fraud, disruption to users, loss of service, damage to the national interest or to the process of good government.

5.3. The implementation stage of all new and replacement computer systems must include the provision of cost effective security measures to counter any risks identified by the risk analysis.

5.4. IT System Managers and information asset owners will implement appropriate counter-measures in the light of the risk assessment.

6. RISK MANAGEMENT ACCREDITATION DOCUMENT SETS

6.1. Every major new or replacement IT system must have a Risk Management and Accreditation Document Set (RM-ADS). It should cover areas such as the scope of the system, the security requirements, standards for security measures, and responsibilities for security aspects.

6.2. The policy should incorporate a synopsis of the risk analysis and, where appropriate, require security operating procedures (SyOps) to be prepared and made available to all those with responsibility for managing the system.

6.3. Accreditation of the RM-ADS is given by the DfT's DSO, through the ITSO. Further information on the RM-ADS and the accreditation procedure is available from the IT Security team.

7. CONTINGENCY PLANNING

7.1. IT system managers must develop appropriate, cost-justified, disaster recovery and contingency planning procedures for all major Company IT systems. Further details are available from the Information Management Group within the CIO Office.

7.2. Once established, these recovery procedures shall be tested and rehearsed as necessary at regular intervals, and at least once a year.

7.3. The use of HMG Information Assurance (IA) Standards is recommended for complex IT systems processing OFFICIAL information.

8. LEGAL REQUIREMENTS

8.1. The use of information is subject to the following legislation:-

8.1.1. **Copyright, Design and Patents Act 1988** - provides the same rights to authors and owners of computer software as that enjoyed by the authors of artistic works. It prohibits the copying or adaptation of software without the authority of the copyright holder;

8.1.2. **Computer Misuse Act 1990** - combats unauthorised access and unauthorised modification of computer material;

8.1.3. **Data Protection Act 1998** - regulates the use of personal data held on a computer and other filing systems, and specifies rules for the way in which the data is obtained and used, to protect the privacy of personal information;

8.1.4. **Public Records Act 1967** - provides for the management of records (including those held on IT systems) of any and all business carried out by government; and

8.1.5. **Official Secrets Acts, 1911-1989** - creates the offence of disclosing official information in six specified areas if the disclosure is damaging to the national interest.

8.1.6. **Freedom of Information Act 2000** – gives the public access to certain defined categories of information stored on paper or IT systems.

8.1.7. Human Rights Act 1998 – governs the means the Agency may employ to monitor staff use of IT systems.

8.2. All use of information within Highways England will conform to the provisions of the legislation to the extent that it is applicable to the Company's work.

9. AUDIT AND COMPLIANCE MONITORING

9.1. The ITSO will monitor and review IT security policies, standards and procedures to ensure that they remain relevant and effective.

9.2. The ITSO will ensure that arrangements are in place to monitor compliance with IT security policy, standards and procedures, together with the assistance of Internal Audit as necessary.

9.3. Non-compliance with the IT security policies, standards and procedures will be treated as a disciplinary offence and referred to line management to be handled in accordance with the disciplinary procedures set out in the Highways England Staff Handbook.

9.4. The ITSO will report annually to the SIRO, the Management Board and to the Departmental ITSO on the adequacy of IT security arrangements for the protection of the confidentiality, integrity and availability of Highways England's IT systems.

9.5. The Agency Records Officer, supported by AICD, will ensure that Document Management policies are implemented throughout the Company. The Data Protection Officer ensures that the Company is DPA compliant.

10. EDUCATION AND AWARENESS

10.1. All Agency staff must have access to security education material and training to familiarise them with the laws governing the use of computers, the IT security procedures they are expected to follow to keep their data and the IT systems they use secure, and the correct use of IT facilities.

10.2. The ITSO is responsible for organising the Company's overall IT security education programme and making training material available. The IT Code of Practice is designed to address this requirement, supplemented with IT security awareness training sessions and the use of the appropriate IT security documents stored on the Highways England document retrieval system (the Portal).

10.3. The requirements for security training for individual IT Systems are the responsibility of their system owners.

10.4. All new permanent and casual Highways England staff should attend an Induction Session including advice on IT Security Policy and procedures with their line manager as soon as practicable.

10.5. The Highways England Records Officer is responsible for promoting awareness of correct Document Management procedures across the Company. The Company Records Officer is supported by the Data Protection Officer and the FOI Officer, who are responsible for promoting compliance with Information Rights Legislation.

11. INCIDENT HANDLING

11.1. Details of all incidents resulting in a breach of IT security, whether by staff or others, and whether deliberate or accidental, must be reported to the ICT Service Desk or direct to the IT Security Team as soon as possible after the event.

11.2. An IT security incident is deemed to occur whenever the confidentiality, integrity or availability of a system is breached (or could have been breached), intentionally or accidentally, and results or could have resulted in an "adverse impact", such as disruption of activities, embarrassment to the Company, financial loss, legal obligation or penalty, threat to personal safety, threat to privacy.

12. THE GOVERNMENT SECURITY CLASSIFICATION POLICY

12.1. Levels of protection and Protective Markings

12.1.1. There are three security classifications described in the Government Security Classification Policy, OFFICIAL; SECRET and TOP SECRET. It is anticipated that virtually all our information will sit in the OFFICIAL classification.

12.1.2. It is the sensitivity of the information that decides how you should classify, handle, store and transmit it.

12.2. Application of Protective Markings

12.2.1. Information assessed as OFFICIAL does not require marking.

12.2.2. Any information that is assessed as being of a significantly sensitive nature should be marked OFFICIAL-SENSITIVE. A caveat may be applied to determine the kind of sensitivity, so for example OFFICIAL-SENSITIVE PERSONAL or OFFICIAL-SENSITIVE COMMERCIAL. These classifications must be clearly visible on the document itself, either as a watermark, or in the heading or clearly included in a footnote, so that if it is printed off the marking can still be seen on the hard copy. The marking should also be clearly marked on the description of documents either as part of the file name, if electronic or on the cover of the folder for paper documents.

12.2.3. The policy anticipates the use of OFFICIAL-SENSITIVE as a classification will be limited to a very small amount of information that requires a higher level of handling protection than most of what we handle every day.

Levels of Protection and Security Classification

Classification	Examples
OFFICIAL	The majority of information that is created or processed by the public sector falls into this category. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile. No marking need be physically applied. • Day to day business of government, service delivery and public finances • Public safety, criminal justice and enforcement activities • Commercial interests, including information provided in confidence and intellectual property • Routine international and diplomatic activities • Many aspects of defence, security and resilience • Personal information that requires protection under the Data Protection Act (1998) or other legislation (e.g. health records)
OFFICIAL-SENSITIVE	If you deem the information to have sufficient sensitivity that it requires additional handling controls to be put in place to give additional protection, mark it OFFICIAL-SENSITIVE. Sensitive corporate or operational information e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues. Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court proceedings Sensitive personal data e.g. health records, financial details, that it is not considered necessary to manage in the SECRET tier Policy development and advice to ministers on contentious and very sensitive issues More sensitive information about defence or security assets or equipment Commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed

SECRET	It is unlikely that we will produce information in this classification, although there may be occasion when it may have to handle it from external agencies. In these circumstances please contact the IT security advice team. Information with a SECRET classification is comprised of very sensitive information that justifies heightened protective measures to be deployed to defend against a determined and highly capable threat actor, e.g. where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
TOP SECRET	It is highly unlikely that we will either produce or have access to information in this category. In these circumstances please contact the IT security advice team. Information in the TOP SECRET classification is the HMG's most sensitive information, requiring the highest levels of protection against the most serious threats, e.g. where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

14. RECORDS POLICY: PAPER AND ELECTRONIC RECORDS

14.1. Everyone has a responsibility to maintain a good record of their work and activity which is readily accessible. The Public Records Act sets out the requirements for the management of all public records throughout the information lifecycle. This means that when information is created, it is only stored in official record keeping systems. Within Highways England we use SHARE for much of our electronic information. We also use databases for a broad range of information, Outlook for transient information and registered files for hard copy documents, although these practices will diminish as electronic records become the norm within the SHARE environment. If you do not store your information in one of these repositories, then it is not being kept in an official record keeping system. Further advice may be obtained from the Highways England Records Officer via the Records Management Advice box in Outlook.

14.2. Good information management means understanding the value of the information you are creating, who can access it and how long it should be kept. It is important to treat all information as a corporate asset and take steps to ensure it is exploited to its full potential, within legal boundaries, for the benefit of our organisation. All records kept either in paper or electronic format will conform to the prevailing policies and procedures available on the Information Management and IT Security pages on the Portal.

ANNEX A

GLOSSARY

(Risk Management) Accreditation Document Set:- A statement of the security requirements and countermeasures applicable to an IT system. It will describe the scope of the system, the security requirements, the standards for security measures and the responsibilities for security aspects.

Contingency Planning:- Identifying the most likely failures that could affect the continuity of essential business operations and services that are dependent on IT, and defining effective plans of response should those failures occur.
Hardware:- Generic name for computers, printers and other devices within an IT system.

IT Security Incident:- Any incident that is likely to affect the confidentiality, integrity or availability of computer information or systems.

IT System:- An integrated assembly of computer data storage, programs and manual operating procedures designed for a purpose. IT systems may operate within or across each other. For example a computer together with its operating system and software packages is an IT system. An application system running on one or more computers is also an IT system.

IT System Manager:- The person charged by the IT System Owner with the day-to-day operational management of an IT system.

IT System Owner:- The person responsible for an IT System who has authority to agree changes to the operation of or to discontinue operation of the system.

IT User:- Any person who actually uses an IT system.

Government Security Classification Policy:- HMG's classification scheme for identifying the sensitivity of government information, for paper based and IT systems.

Security Operating Procedures (SyOps):- These provide details of how the IT system will be operated and maintained in a secure manner in line with the requirements of the SSP.

SHARE (Sharing Highways Agency Records Electronically):- The Company's default system for storing electronic information.

SIRO (Senior Information Risk Owner) – individual responsible for the control of information risk across the Company's information systems.

Software:- Generic name for the application programs, operating system and other programs within an IT system.

ANNEX B

CONTACTS

IT Security Officer

Victoria Williams, 4 South, Lateral	TEL: 5173 5366

IT Security Administrator

Harry Payne, 4 South, Lateral	TEL: 5173 6818

Data Protection Officer:

Sian Jones, Piccadilly Gate	TEL: 4315 5541

FURTHER GUIDANCE

IT Security Standards	SHARE link
Password Construction Guide	SHARE link
Data Handling Policy	SHARE link
Mobile working Security Operating procedure (SyOps)	SHARE link