Information Security Policy

Operational Technology Security

MCH2610

Date: 01/09/2016 **Version 1.0**

Registered office Bridge House, 1 Walnut Tree Close, Guildford GU1 4LZ

0 Document Control

Document Title	MCH2610 – Information Security Policy
Author	Jenny White
Owner	Operational Technology Security
Distribution	Highways England
Document Status	Issued

0.1 Revision History

Version	Date	Description	Author
V0.1	19 August 2016	First review	Charles Spencer
V0.2	24 August 2016	Second Draft	Charles Spencer
V0.3	24 August 2016	Final Review	Charles Spencer
V1.0	01 September 2016	First Issue	Jenny White

0.2 Approvals

Version	Date	Name	Title	Signature
V1.0	31 August 2016	Jenny White	OT Security Manager	
V1.0	31 August 2016	David Bradbrook	OT Strategic Director	

0.3 SIRO approval

As Highways England Senior Information Risk Owner (SIRO), I can confirm that I am ultimately responsible for managing Information Security Risk on behalf of the organisation. I am satisfied that this policy enacted by Operational Technology Security is appropriate for managing the security of Operational Technology.

Version	Date	Name	Title	Signature
V1.0	31 August 2016	Vanessa Howlison	Highways England SIRO	

0.4 Glossary

Description	Definition
Operational Technology	As described in ITD OT Strategy (noun).
Information Security	The act of protecting a business' information (verb).
Information Assurance	The act of confirming protection of a business' information (verb).
Data and Information	Refer to pure information as described by CESG.
Information Assets	Refer to hardware, software and pure information (data).
Confidentially	Indicates limiting access to information assets.
Integrity	Indicates the legitimacy and completeness of information assets
Availability	Indicates the readiness and accessibility of information assets.
Impact	Indicates the consequence or possible consequence
Threat	The cause of a risk
Vulnerability	The source of a risk
Assessment	The act of qualifying and quantifying technical and business risk.
Treatment	An act of managing business risk.
Gross Risk	An assessment of risk made before treatment has been implemented.
Net Risk	An assessment of risk made after treatment has been implemented.
Appetite	A statement of acceptability
Escalation	A procedure to accept risk that is managed but unacceptable.
Quality and Assurance	The act of an internal review that ensures the quality of output
Personal information	Information assets or information assets combined with other information held or soon to be held by the data controller that can identify or locate an individual
Sensitive personal information	Personal information consisting of racial, ethnic origin; political opinions; religious or cultural belief; physical or mental health; sexual life; the commission or alleged commission of any offence; membership of a trade union (Trade Union and Labour Relations (Consolidation) Act 1992); and, proceedings for any offence committed or alleged to have been committed and including the disposal of such proceedings or the sentence of any court in such proceedings.
Classification	Official, Secret and Top Secret as described in UK Government Security Classification (2014).

Table of Contents

1 Introduction

Operational Technology Security (OTS) assesses the risk to the confidentiality, integrity and availability (CIA) of Operational Technology (OT) deployed on the Strategic Road Network (SRN). The team is positioned in the Information and Technology Directorate (ITD) and operates alongside Highways England Business Information Technology (HAbIT), the National Resilience and Security Team (NRST), Highways England's Data Protection Officer (DPO) and reports to Highways England Senior Information Security Officer (SIRO).

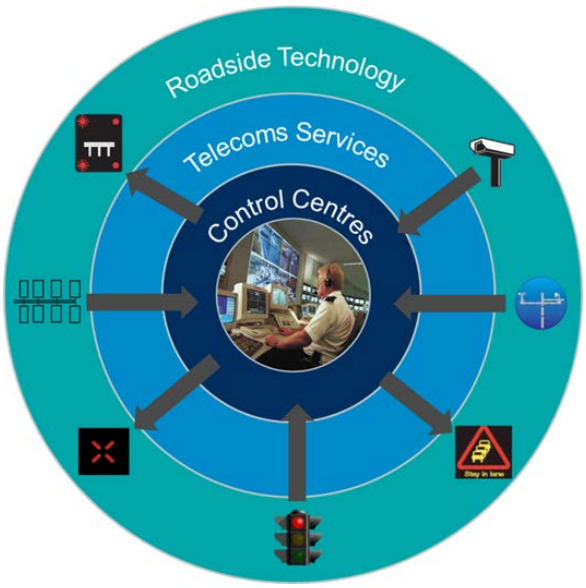
1.1 Purpose

This document describes the Information Security Management System (ISMS) and security products that will govern, manage and assure the CIA of OT deployed on the SRN and, in doing so, described how OTS will achieve the security objective described in the Highways England OTS Strategy.

1.2 Scope

OT is the term used to describe the technology that enables us to operate and monitor the SRN. OT is categorised into the following areas:

- **Roadside Technology** - technology deployed at the roadside (signs, signals, CCTV cameras etc.).
- **Telecoms services** - the systems and services that interconnect the roadside technology with the control centre systems.
- **Control Centres** - centralised systems that are used to monitor and control the roadside technology.



2 Requirements

2.1 Legislation and regulation

OTS and its ISMS will comply with all UK Legislation, original or revised as published in the National Archives and, not limited to legislation pertaining to information security or data privacy. OTS and its ISMS is regulated by the mandatory security outcomes described in HMG Security Policy Framework [Ref A] and will apply protective security to ensure Highways England can function effectively, efficiently and securely.

As defined by the Independent Commissioners Office (ICO), Highways England is defined as a Data Controller and Data Processer of personal and personal-sensitive information. In accordance with the ICO, OTS will defer to the Highways England DPO when such information is to be stored or processed by OT.

2.2 Business strategies

OTS and its ISMS will support the realisation of strategic objectives described in the UK Government Cyber Security Strategy [Ref B] and the strategic outcome described in Highways England's Strategic Business Plan (SBP).

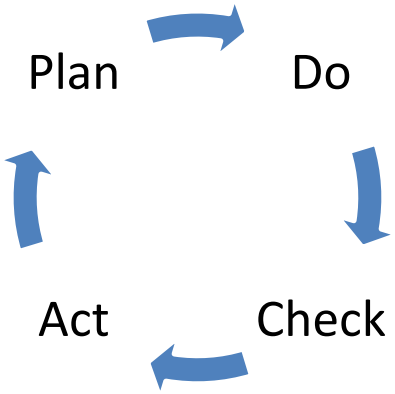
The OTS Strategy will translate the business requirements described in the Highways England Delivery Plan [Ref C] into OTS objectives. Each OTS objective will be managed by a campaign plan that details how OTS and ISMS will mature by 2020; each campaign plan will leverage our approach as described in Highways England OT Strategy. The OTS Strategy will be the primary and authoritative source of direction for formulation and review of OTS ISMS.

2.3 Current and projected threat environment

OTS will collaborate with the Centre for the Protection of National Infrastructure (CPNI) and CESG – the Technical Authority for Information Assurance. These partnerships will enable information exchange and the formation and maintenance of an environment-specific and Department for Transport (DfT) authorised threat model. In utilising a threat model, advice from the ICO and the UK Government Security Classification [Ref D], OTS will identify requirements determined by the threat environment.

3 Approach

OTS will employ a Plan, Do, Check, Act (PCDA) cycle as an overarching approach to maintaining and implementing its ISMS. OTS will also ensure an internal quality and assurance (Q&A) mechanism compliments the approach; the Q&A mechanism will enable OTS to adapt output to agile environments.



OTS will categorise its ISMS into Governance, Risk Management, Compliance and Support policies, procedures and activities. This will better enable supply and demand modelling and support leadership decision-making.

3.1 Governance

OTS will use a three tier governance and management structure to ensure risk management, compliance and support activity across Highways England's value chain is effective, prioritised and demand is mapped to resource and capability, see *Table 1*.

No.	Tier Name	Details:
1st	**OT Security Steering Group**	**Chair:** OT Security Manager **Required:** OT Security **Optional Attendees:** Highways England SLT, OT Security partners **Frequency:** Monthly **Input:** ISWGs output, Business ICT, NRST and DPO actions. **Output:** Register / tracker updates, supply and demand modelling and reporting.
2nd	**Information Security Working Groups**	**Chairs:** OT Security Analyst **Required:** Relevant members of the Security Community **Optional Attendees:** Highways England SLT **Frequency:** adhoc e.g. as required by a Code of Connection Application **Input:** Security Community output e.g. Supplier IASG and IAWG **Output:** e.g. security reports, task allocation, requirements.
3rd	**Security Community** **e.g. NRTS, NTIS, Supply Chain**	**Chair:** A member of the Security Community **Required:** Relevant members of the Security Community **Optional Attendees:** OT Security analyst **Frequency:** driven by business and security requirements **Input:** e.g. communications and awareness publications, vulnerability analysis. **Form:** e.g. Supplier IASG and IAWG.

Table 1 – OTS three tier governance and management structure

3.1.1 Reporting

OTS will attend the Security and Business Continuity Group chaired by Highways England SIRO. This group meets every quarter and will measure the effectiveness of OTS ISMS, submitting an annual Statement of Internal Control to DfT. OTS will submit monthly Highlight Reports to Highways England's SLT; this will include details on risks and issues to the effectiveness of OTS and its ISMS.

3.2 Risk Management

OTS will employ a risk-based approach to security and assess the impact of compromised CIA against achieving business requirements described in the Delivery Plan.

MCH2613 – Risk Management Policy [Ref E] will describe the risk appetite, risk assessment methodology and the algorithm used for selecting security controls from an Enterprise Security Architecture (ESA). Output from conducting risk management will be recorded in an application as informed by the MCH1514 – Risk Management Procedure [Ref F]. This procedure will be approved by DfT and required for all OT that is to be deployed on the SRN. Each application will form a record and its accompanying Risk Register will form a live document; the Risk Register will be technology agnostic but inform a defined Risk Summary Statement and risk escalation mechanism.

The industry and best practice standards forming the ESA will be:

- CSA - Security Guidance for Critical Areas of Focus in Cloud Computing [Ref G].
- CPNI - The Critical Security Controls for Effective Cyber Defence [Ref H].
- CESG – Cloud Security Guidance [Ref I].
- HMG Cyber Essentials Scheme [Ref J].
- ISO27001:2013 [Ref K] and ISO27002:2013 [Ref L].

3.2.1 Reporting

OTS will report security risks to Operational Technology via a monthly Risk Summary Statement to Highways England SIRO. OTS will also maintain an escalation mechanism to report security risks above OT Risk Appetite Statement (OTS RAS), in order to enable business.

3.3 Compliance

The prescribed risk management process will also detail a consistent and transparent formula that OTS will use for selecting levels of assuring OT. The levels of assurance will be aligned to the guidance on implementing the CESG – Cloud Security Principles [Ref M]:

- Self-assertion.

- Contract agreement.
- Independent assertion.
- Independent testing.
- Assured design.
- Assured components.

In order to secure OT over its lifespan and assist in through-life support (OT maintenance), OT Security will formulate and implement:

- An audit procedure.
- Code of Connection Application reviews.

OTS will assist Highways England's Project Sponsors and their suppliers' compliance to other Government department security requirements and conditions.

3.4 Support

OTS will develop a number of subordinate policies and artefacts to support this policy and those aforementioned:

- An asset disposal policy.
- A cryptography management policy.
- An incident security management policy.
- Communications Guidance, inclusive of training and awareness.
- A Technical Vulnerability Management procedure.
- An ISMS Manual.
- A task and activity trackers.

OTS will review each ISMS document annually; updated documents will be recorded in Highways England's Plans Registry.

4 OTS Structure

To generate efficiencies and for economy of effort, OTS will employ a core team of analysts and provide OT projects with security advice/requirements or, embedded support if required by the business. Each individual will be accountable to and line managed by the OT Security Manager; Highways England's project sponsors will support the OT Security Manager as required. The Skills for the Information Age (SFIA) framework will be used to prescribe the required competence of each role:

4.1 OT Security Manager

SFIA 4/5:

- Authorise OTS activity and priorities.
- Govern the process of Risk Management.
- Maintain the risk register and ISMS trackers.
- Line management of OTS.
- Influence relationships with internal and external SLTs.
- Maintain the relationship with Department for Transport (DfT).

4.2 OT Security Lead Analyst

SFIA 4:

- Establish and maintain the ISMS.
- Prioritise and record OTS output.
- Allocate resources.
- Operational management of OTS analysts.
- Risk management and compliance for complex systems.
- Influence relationships with internal and external SLTs.

4.3 OT Security Analyst

SFIA 3

- Schedule and conduct risk management, compliance and support activity.
- Conduct Q&A on OTS activity output.
- Establish and influence relationships with internal stakeholders.

4.4 OTS peripheral team

SFIA 3 or 4:

- Operational Management as required by the business or project sponsors.
- Risk management and compliance as dictated by operational management.
- Influence relationships with internal and external SLTs.

5 Department for Transport

The OT Security Manager will liaise with DfT and gain their approval for risk management using the process described in Section 3.2 of MCH2610. OTS will maintain an informal and formal relationship with DfT for the purpose of risk management and management of government information.

6 Feedback and enquiries

Users of this document are encouraged to raise any enquiries or provide feedback on its content and usage to OTS. The email address for all enquiries and feedback is: OTSecurity@highwaysengland.co.uk

7 Informative references

Where a version is not explicitly specified, the latest published version should be assumed.

A. HMG, Security Policy Framework, Cabinet Office.

B. UK Government, Cyber Security Strategy, Cabinet Office.

C. Highways England, Delivery Plan 2015 – 2020, Highways England.

D. UK Government, Government Security Classification, Cabinet Office.

E. OTS, MCH2613 – Risk Management Policy, Highways England.

F. OTS, MCH1514 – Risk Management Procedure, Highways England.

G. CSA, Security Guidance for Critical Areas of Focus in Cloud Computing.

H. CPNI, The Critical Security Controls for Effective Cyber Defence.

I. CESG – Cloud Security Guidance, UK Government.

J. HMG, Cyber Essentials Scheme, UK Government.

K. ISO/IEC 27001:2013 – Information Security Management Systems, BSI.

L. ISO/IEC 27002:2013 – Code of Practice for Information Security Controls, BSI.

M. CESG, Cloud Security Principles, UK Government.

END OF DOCUMENT