OFFICIAL

highways england

INFORMATION SECURITY

INCIDENT MANAGEMENT REQUIREMENTS

Document Purpose
This document details the management of Information Security incidents

cybersecurity@highwaysengland.co.uk

1 Document Control

Document Title	Incident Management Requirements
Author	Jenny White
Owner	Information Security
Distribution	Highways England
Document Status	Issued

1.1 Revision History

Version	Date	Description	Author
1.0	13 Oct 2015	Initial Release	David Goddard
2.0	11 Feb 2019	Rework as part of CDO initiative document reviews	Simon Andrews
2.1	22 Feb 2019	Minor formatting and additions.	Scott Bartlett
2.2	14 Mar 2019	Minor Formatting	Scott Bartlett
2.3	03 July 2019	Alterations following review by Jenny White	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		2.3

DRAFT

This document is copyright to Highways England.

2 Overview

These requirements define how Information Security Incidents and Weaknesses within Highway England (HE) shall be managed through-life from initial response to lessons learned.

Whilst every effort can be made to secure a system and environment, there will be incidents whether internal, external, deliberate or accidental that compromise "security". It is therefore necessary to ensure procedures are in place so that security events and incidents are responded to in the correct manner including reporting, investigation and corrective actions. Similarly, vulnerabilities, also known as weaknesses or 'near misses' will be observed from time to time.

3 Who Should Use This Document

This document shall be used by service delivery managers and where appropriate suppliers to enable local translated versions of this requirements document.

4 Information Security Map

The below diagram illustrates where this document sits within the broader information security system (ISS) of documents.

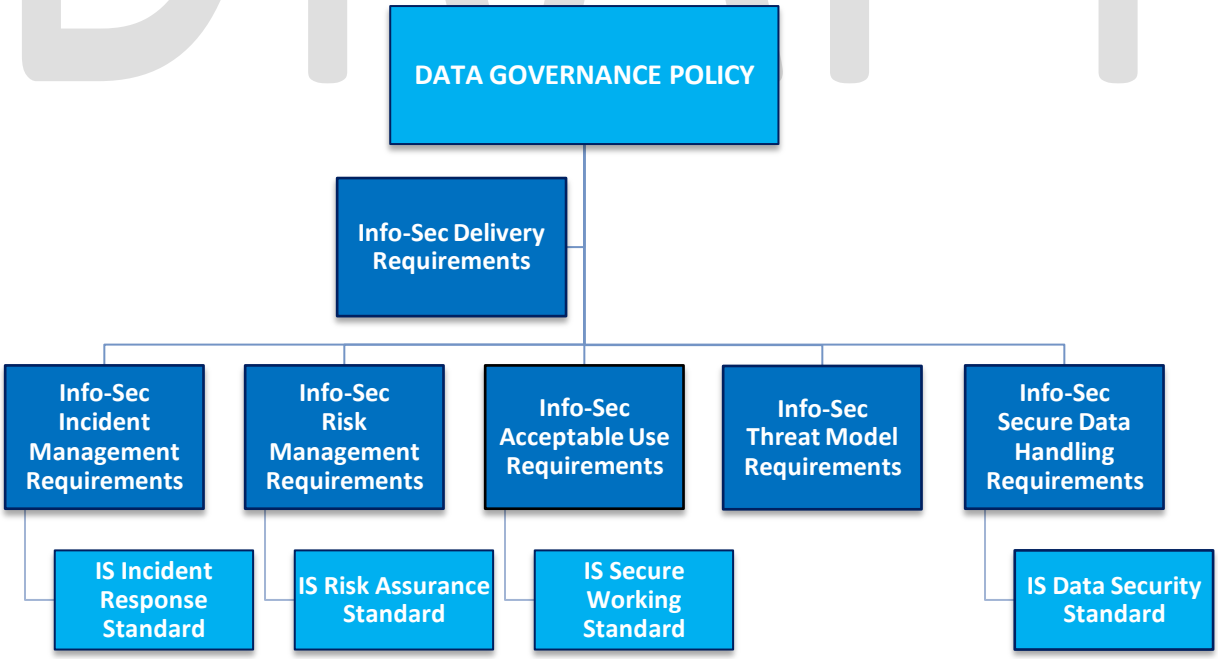

Figure 1 – Information Security System (ISS)

DRAFT

This document is copyright to Highways England.

5 Contents

1 Document Control 2
2 Overview 3
3 Who Should Use This Document 3
4 Information Security Map 3
5 Contents 4
6 Definitions 4
7 Scope 5
8 Intended Audience 5
9 The CMM and Information Security Incidents 5
10 Incident Management Roles and Responsibilities 6
11 Incident Management 7
12 Identifying Information Security Incidents 8
13 Communicating Information Security Incidents 8
14 Incident Classification 9
15 Investigation Management Actions 10
16 Compliance 11
17 Contact Us 11

DRAFT

6 Definitions

Information System – 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 Security Event – An Information security event indicates that

- The security of an information system, service, or network may have been breached or compromised.
- An information security policy may have been violated or a safeguard may have failed.

Information Security Incident – An information security incident is made up of one or more unwanted or unexpected information security events that could very likely compromise the confidentiality, integrity or availability of information and weaken or impair business operations

GDPR – The General Data Protection Regulation is a EU wide law governing how data identified as personal identifiable data should be managed.

This document is copyright to Highways England.

NIS – The Network Information System directive is an EU wide set of rules around information security that apply to certain areas of Highways England.

7 Scope

The requirements apply across the entire HE environment and are in accordance with the Highways England Crisis Management Manual (CMM). Any information security incident that is identified by Highways England Information Security as above the CMM defined routine operations category shall activate the CMM process.

8 Intended Audience

This document is to be read by all managers across all areas of Highways England. All Personnel are to be aware of the requirement to report any information security incident to Highways England line management or a member of the Highways England Information Security team.

DRAFT

9 The CMM and Information Security Incidents

The mapping between Information Security Incidents categories and the general categories of incident within the CMM are defined in the figure below.

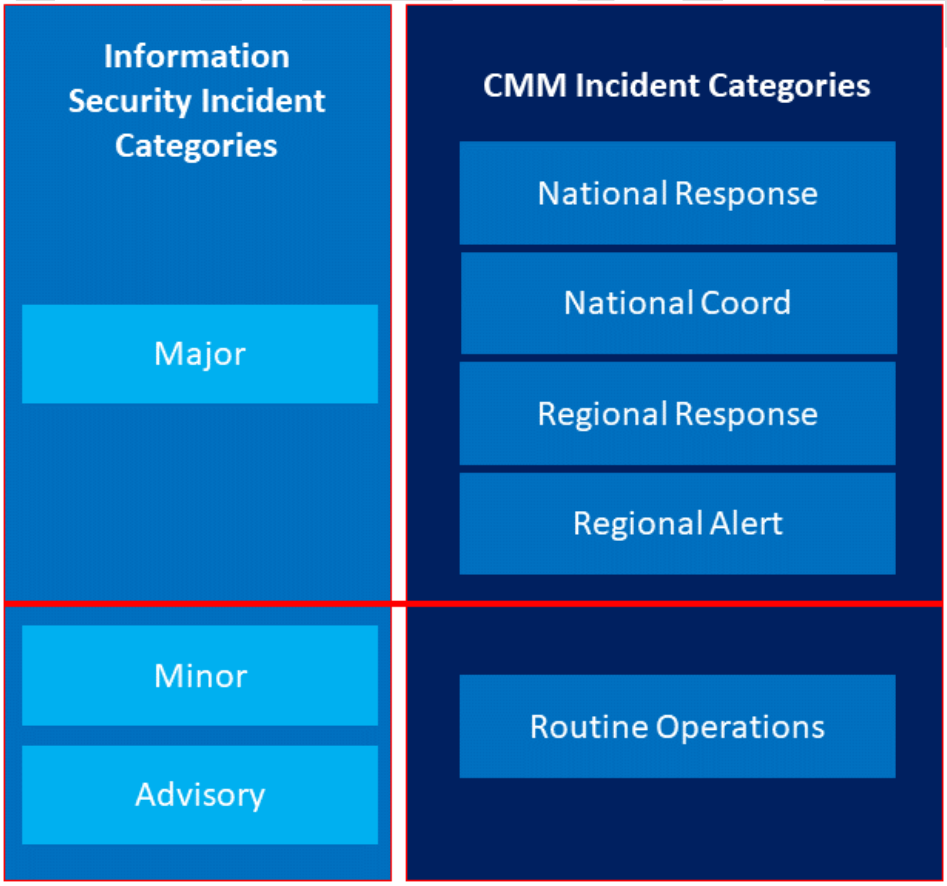

Figure 2 – CMM Mapping

This document is copyright to Highways England.

10 Incident Management Roles and Responsibilities

10.1 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for all risks to information and systems at Highways England.

10.2 Information Security Team Manager

The Highways England Information Security Team Manager shall act as the point of contact and shall be responsible for the management of information security incidents and vulnerabilities affecting Highways England where they fall under Routine Operations, as defined in the CMM.

10.3 Project sponsor/Service Delivery Managers

Project sponsors and service delivery managers shall be responsible for ensuring suppliers of systems manage and implement recommendations to resolve an incident, as well as managing risk.

10.4 National Resilience and Security Team

NRST manage the content of the CMM. In the event that an information security incident is assessed to have a greater impact than Routine Operations, NRST shall be responsible for coordinating the activities in response to the incident in line with the CMM and through a Duty Crisis Management Coordinator (CMC).

10.5 National Incident Liaison Officer

The National Incident Liaison Officer (NILO) shall be responsible for maintaining an overview of all network incidents and shall escalate an incident to the Duty CMC where appropriate.

10.6 Emergency Response Team

The Emergency Response Team (ERT) shall be responsible for coordinating the crisis management activity within the region, advising on appropriate escalation stage, reporting and meeting schedule.

10.7 Highways England Information Security

Highways England Information Security shall manage the full lifecycle of information security incidents considered as Routine Operations in the CMM. They shall also provide specialist assistance to the NRST for information security incidents that are escalated above Routine Operations.

10.8 Other stakeholders

Highways England Information Security shall inform the Public-sector Network Authority and National Police Information Risk Management Team of any incidents on systems that are connected to the Public-sector Network.

DRAFT

This document is copyright to Highways England.

11 Incident Management

11.1 Overarching Requirements

The following controls shall be implemented across Highways England business areas responsible for the delivery or management of information systems:

a. Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

b. Information security events shall be reported through appropriate management channels as quickly as possible.

c. Employees and contractors using the organisations information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

d. Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents.

e. Information security incidents shall be responded to in accordance with the Highways England Crisis Management Manual (CMM) and any local documented procedures.

f. Knowledge gained from analysing and resolving information security incidents shall be used to reduce the impact or likelihood of future incidents. This information shall be captured in the designated section on the Information Security Incident Response Standard reporting form.

g. The business unit shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

h. The report form detailed in the Information Security Incident Response Standard shall be completed to support the information security incident management process.

DRAFT

This document is copyright to Highways England.

12 Identifying Information Security Incidents

12.1 Definition

Information Security incidents can arise from a variety of sources and come in many different forms including system alerts through to personal observation.

An information security incident is any information security event or collection of events that has, or may, compromise the confidentiality, integrity and/or availability of any asset (physical or technical) across the entire HE environment including IT networks and systems through to documentation, facilities and assets that support personnel and processes in achieving the HE mission. The terms confidentiality, integrity and availability are defined below.

12.1.1 Confidentiality

Confidentiality is the requirement that information and assets must only be accessible to those that are authorised

12.1.2 Integrity

Integrity is the requirement that information and assets must be accurate and complete

12.1.3 Availability

Availability is the requirement that information, assets and services are to be accessible in a timely manner.

13 Communicating Information Security Incidents

In any case where there is an immediate danger to life, either your own or another person then safeguarding individuals' safety takes precedent over any requirements of information security incident management.

If it has been determined using the criteria above that an information security incident is or is about to occur, then users must immediately notify:

Cybersecurity@highwaysengland.co.uk

DRAFT

This document is copyright to Highways England.

14 Incident Classification

There are three classifications that Highways England use to identify an incident. these are:

14.1.1 Advisory

An advisory incident is the communication of a technical vulnerability or significant change in the threat landscape that requires immediate attention. It is separate to the other incident classes in that nothing adverse has happened rather there is an exponential increase in the threat agent hostile intent or a severe technical vulnerability that is present across large or critical areas of the Highways England estate.

Information security receive both critical patch news from major suppliers but also perform regular open source analysis of publicly available exploits and shall reach out to relevant points of contact where appropriate to begin remediation.

14.1.2 Minor incident

A minor incident is an isolated event which could compromise the confidentiality, integrity or availability of a non-critical Highways England system at a local level. Local in this context means a sub-set of users that access a service.

14.1.3 Major Incident

Any incident that is, or suspected to be one of the following:

- Where it is assessed the incident is a concerted, repeated and targeted effort by a threat agent.
- Where it is assessed to impact on the confidentiality, integrity or availability of a Highways England service in its entirety.
- Where the system affected belongs to a service defined as business critical.

DRAFT

This document is copyright to Highways England.

15 Investigation Management Actions

15.1 Assess and Classify

Once alerted to an incident Information Security assess the available information and then classify it as minor or major. This is assessment will attempt to evaluate what is already known and in the case of cyber-attack will not involve any form of system interaction. Using the incident classification metrics defined earlier the incident is then classified and minor or major.

Major incidents will require escalation and shall follow the procedures defined in the Highways England ***Error! Reference source not found.*** *(CMM).* Where this is the c ase Information Security will advise and inform before handing over incident control to the relevant person defined in the CMM.

15.1.1 Contemporaneous Logging

Information security maintain a security incident tracker to enable the appropriate investigation, reporting and follow on actions of any security incident. This log must be filled out during the investigation so that all actions are auditable, this log includes all communications and decision points. The log is then able to provide an accurate and centralised reporting mechanism that shall be used to brief other areas of incident management across the business such as other members defined in the CMM.

15.2 Report and Respond

1. Upon classification if appropriate the Chief Data Officer (CDO) and National Resilience and Security Team (NRST) is consulted and appropriate actions within the CMM are enacted.

2. An incident working group shall then be established between Information Security, incident reporters and relevant points of contact defined by the incident size.

This working group shall then establish a series of actions that must be taken in the immediate term (24 hours) to decide any legal reporting requirements, safeguard evidence, restore functionality and limit potential impact. Where this involves potential criminal activity, senior leadership shall be informed and actions taken in-line with their guidance.

Where legal reporting requirements related to GDPR are identified Highways England Senior Leadership Team (SLT) must take the ultimate decision as to whether an incident must be reported.

Where legal reporting requirements relating to the NIS directive are identified, the decision to report the incident must be made at the C level management position, preferably by the Chief Information Security Officer (CISO).

This document is copyright to Highways England.

3. In the medium term (1-2 weeks) the following define more granular activities that must be achieved by the security working group:

- Identification of the root cause of the Information Security Incident;
- Identification of any contributory factors that led to the Information Security Incident;
- Identification of actions to prevent/mitigate recurrence of the information security incident.

15.2.1 Evidence Collection

Digital evidence collection is an ever-evolving science that requires specialist tools and training. Whilst the Information Security Team can interpret some information during an incident where a malpractice is suspected either accidentally or maliciously then no effort should be made to interact with the system/data in question other than if there is an immediate threat to safety or the security working group decide that system operation and functionality takes priority. Where evidence is required to be collected specialist persons must be brought in to ensure permissible evidence is collected and preserved. This must follow guidance defined in the latest version of the association of chief police officers good practice guide for digital evidence.

15.3 Recover and Understand

Upon resolution of an incident the Information Security Incident lead must complete a security incident summary report. This report is detailed in the Information Security Incident Report Standard. Valuable lessons can be learned from investigations and all information security incidents should be fully assessed to identify these lessons.

16 Compliance

Information security retain the right to audit a solution to ensure that post-incident corrective actions have been implemented which successfully remediate the incident and that preventative measures put in place ensure that the incident is less likely to occur in the future.

If it becomes apparent that a solution has not adequately completed its security responsibilities or new threats emerge which compromise the confidentiality, integrity or availability of an existing solution, the risk will be assessed in line with the Information Security Risk Management Requirements and the Information Security Risk Assurance standard.

17 Contact Us

For errors, omissions and general queries email:

cybersecurity@highwaysengland.co.uk

This document is copyright to Highways England.