This policy draws together all information policies which help us manage information in accordance with the relevant legislations and regulations which apply. Information assurance is the practice of managing risks relating to the use, processing, storage and transmission of information or data. All systems and processes used to enable this to happen have to be in line with our corporate policies.

Introduction

This policy establishes our commitment to information assurance. It aims to assure our information assets through a risk-based, proportionate framework of controls to:

- Deliver confidentiality of information, by protecting assets against unauthorised disclosure;
- Preserve information integrity, by protecting assets from unauthorised or accidental modification;
- Maintain availability of information, by ensuring that assets are accessible as and when required by those authorised to do so;
- Deliver compliance with all legal and statutory requirements;

All the policies listed below apply to all our information assets, whether managed directly by Highways England, or by a contractor on behalf.

All the policies listed below apply to all members of staff and anyone who may process information on our behalf.

Relevant legislation

We will comply with all legislation and statutory requirements relevant to information and information systems, including, but not limited to:

- Computer Misuse Act 1990;
- General Data Protection Regulation (GDPR) (EU) 2016/679
- Communications Act 2003;
- Public Records Acts 1958 and 1967
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004
- Re-Use of Public Sector Information Regulations 2015

Compliance will be managed through the implementation of the policies below.

Managing the risk

A risk assessment process shall maintain:

- A corporate information asset register;
- Regular inventories to:
  - Determine the existence, ownership and accountability of information assets, including the classification of information sensitivity;
  - Support the management and resourcing of information assurance activities
    - Information assets shall be secured using controls proportionate to the risks faced by the company.
    - Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

Our Senior Information Risk Owner (SIRO) is the focus for the management of information risk within the company.

Compliance

Managers and information asset owners shall implement all relevant information assurance controls within their area of responsibility to achieve compliance with the information assurance policy.

Compliance with this policy and its subsidiary policies will be supported by:

• Evidentiary reviews, including quality assurance and testing activities;
• Monitoring, auditing and reporting of network and information system activity;

Any breaches of policy, or deliberate non-compliance with policy will be investigated, reported and may be treated as misconduct under the appropriate staff disciplinary policy. Failure to carry out mandatory actions within policy implementation documents may be considered a breach of the relevant policy.

In the event you become aware of a potential breach of this policy, please report your concerns to your manager and the Head of Data and Information Governance. Breaches under GDPR must be reported to the Data Protection Officer immediately they are known about.

.

Information Management Policies

Our information management policies shall be considered part of this policy and shall have equal standing. The list may be added to under governance arrangements detailed above:

1. Data Protection
2. Company Records Policy
3. Clear Desk Policy
4. Scanning Policy
5. Health & Safety Records Policy

6. Retention Policy
7. Data Handling Policy
8. Third Party Records Management (Annex 19)
9. Acceptable Use Policy
10. Information Security Policy
11. Mobile Working
12. Wireless Policy
13. Information Asset Register
14. CIO memos
15. Digital Signatures
16. Digital Continuity Policy