Data Handling Policy for Supply Chains

Purpose

1. This document is an overview of how you and your company should handle information that is owned by Highways England, or owned by your company and used on our behalf, to ensure its security. It covers the use of protective markings, and explains how to use various electronic methods of handling information as well as paper.

Introduction

2. This policy places far greater emphasis on using your own judgment and expertise to protect the information you handle rather than laying down strict instructions for information handling. This allows you far greater flexibility to share information with those who need to know about it.

3. Treating all the information you handle the same way can lead to either wasting resources in over-protecting it, or loss of reputation and/or fines (both for a company and for individuals) in not protecting it enough. The content of the information determines how it is handled and what protection it needs, if any. For example:
   a. Tender documents containing a detailed breakdown on how the tenderer proposes to assign resources to a project and how much they will cost should only be available to people with a need to know the details. The confidentiality of this information is important.
   b. Anonymised traffic flow figures can be shown to anybody both inside and outside the company on request. They are not confidential, but their integrity (accuracy) is important, as is their availability.

Levels of protection and Protective Markings

4. The Government Security Classification Policy sets out protective markings that relate to the sensitivity (confidentiality) of information. They are a warning that special handling may be required.

5. There are three security classifications: OFFICIAL, SECRET and TOP SECRET. A table explaining these classifications is in the “Further Information” section towards the end of this document.

6. In the unlikely event of your handling SECRET or TOP SECRET information on HE’s behalf you will be formally briefed on how this must be done. This document only covers handling of OFFICIAL information.

7. OFFICIAL information does not have to be marked, and it is HE policy not to mark it unless it has particular sensitivity: in which case, it will be marked OFFICIAL SENSITIVE. This will be used only where there is a clear and justifiable need to reinforce the ‘need to know’ principle, when compromise or

loss could have particularly damaging consequences. A private company's equivalent marking would be "Commercial in Confidence" or similar.

8. Any OFFICIAL SENSITIVE information handled by your company will be given specific handling instructions by the Information Asset Owner (IAO). An IAO is an HE employee who is personally responsible for making sure that information is correctly handled by whoever they agree has to handle it.

Paper documents

9. Keep these out of sight when not in use, and lock them away at the end of the day. If they're marked OFFICIAL SENSITIVE, make sure that only those with a "need to know" have the keys to where they're stored.

10. You can post OFFICIAL paper documents, including those marked OFFICIAL SENSITIVE, without any additional protection. You may wish to consider using Special Delivery or other delivery methods that track delivery and require a signature for receipt.

11. If your company has to keep copies of our paper documents for its records you must keep them in an official file which can be tracked and audited.

Company IT

12. We will have agreed with your company that its IT equipment is sufficiently secure to handle our information for work purposes.

13. This security will include basic good practice such as: keeping software patches and upgrades up to date, using the screen lock when moving away from your desk for a short time, and taking care of company laptops when you are working away from the office.

Personal and third party IT

14. You must not use your personal IT equipment, or anyone else's IT equipment other than ours, to handle our information or to access our IT networks.

Removable media

15. We only use removable media for temporary storage and transferring information where a network connection is not feasible.

16. Optical discs (CDs, DVDs, and Blu-Rays) may be used to handle OFFICIAL information. OFFICIAL SENSITIVE information held on optical discs must be encrypted to our standard. This is currently AES 256-bit, using a unique password at least 9 characters long which is not just a single word or a single word with a number tacked on to the start or the end.

17. We only allow specific USB devices on its network and will temporarily issue them to its business partners if needed for data transfer. These devices are encrypted to our standard or higher. If you use your company's USB devices to handle our information marked OFFICIAL SENSITIVE, either the device or the information must be encrypted.

18. You may post removable media to us without any additional protection. You should consider whether all information you are posting using removable is

encrypted even if it is not marked OFFICIAL SENSITIVE. Passwords for encrypted drives or information must not be posted with the removable media.

Online storage and the Cloud

19. Not all online or Cloud storage is secure enough to handle our information. If your company is doing this, it must have been approved in advance by us. In particular, the Cabinet Office guidelines on offshoring must be followed if any aspect of a proposed online or Cloud storage solution, including backups or support at any level, is or may be located outside the UK.

20. Where the Cabinet Office guidelines are not followed in procuring offshore Cloud services, we may demand its information is not held on them.

Email and fax

21. You can email our documents to us, and to other third parties with our agreement, provided they are not marked OFFICIAL SENSITIVE.

22. You must not fax anything marked OFFICIAL SENSITIVE.

Disposal

23. You may dispose of loose paper Highways England documents in your company's recycling bins unless they are marked OFFICIAL SENSITIVE. In those cases, you may either dispose of them in a cross-cut shredder with our approval, or return them to us if requested.

24. You must return our folders and optical discs to us when they are no longer needed.

25. You must return our removable media to our IT security team when you no longer need it. Their address is at the end of this document.

26. You must delete our information from server storage (including cloud storage and any backups) when it is no longer needed or in accordance with any deletion date agreed with us.

Loss or theft

27. Loss or theft of any of our information and where appropriate our media or device it is held on, must be reported to our IT security team as soon as possible.

Exceptions

28. Any exceptions to these procedures must be approved in writing by one of our Information Asset Owners, or a member of our Information Management Team, or our Senior Information Risk Owner.

Review and version handling

29. This document will be reviewed annually, and a revised version issued annually or earlier if necessary.

30. The original version of this document is owned and kept by Highways England. If you are not certain you have the latest version, please email to check.

Further information

Security Classification table

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 the information has sufficient sensitivity that it requires additional handling controls to give additional protection, it will be marked OFFICIAL-SENSITIVE. • Sensitive corporate or operational information eg 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 eg 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	Very sensitive information that justifies heightened protective measures to be deployed to defend against a determined and highly capable threat actor, eg where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
TOP SECRET	HMG's most sensitive information, requiring the highest levels of protection against the most serious threats, eg where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Contact

IT security advice team
Highways England
Lateral
8 City Walk
Leeds LS11 9AT
Email itsecurityadvice@highwaysengland.co.uk

Harry Payne Digitally signed by Harry Payne
Date: 2017.07.10 14:18:30 +01'00'