RMAS - Terms of Use Agreement

1. Information Security Requirements

Information Security is critical to ensuring the protection of Highways England operational capabilities.

This agreement applies to all persons or systems accessing:

- Remote Maintenance Access Service (RMAS)
- Highways England traffic technology systems and services
- Other systems or services connected to the National Roadside Telecommunications Service (NRTS) network

Typically, if you maintain or administer, use operationally or access data from these systems or services, it will be necessary for you to apply for access and sign this agreement.

Highways England reserves the right to withdraw access to systems or services at any time and without notice.

2. Access and accounts

Access to any TTD system or service is normally provided through an account and password or through a digital key/certificate pair and associated pass phrase (hereafter referred to as an "account").

When your account is issued, you will be told for which systems or services the account is authorised along with any limitations to that access.

You agree to observe the following requirements:

- Under no circumstances should you use your account to access a system or service for which the account has not been authorised.
- Accounts and passwords must not be shared.
- Digital keys and Passwords must never be divulged to anyone else.
- Passwords must:
  - be changed regularly – at least every three months;
  - not be common words or names;
  - not be obvious to others;
  - not be recorded (e.g. written down) in a way that would allow another person to easily discover the password;
  - follow the Highways England password policy.

3. Data Security and Confidentiality

Highways England holds the copyright in the data obtained from its systems and services. Data obtained from Highways England systems and services must not be distributed to other persons or organisations without prior written authorisation from Highways England.

4. Network and Service Monitoring

You consent to monitoring and recording of activity on managed networks and services as a condition of using these systems and services.

5. External Connections

You must not connect unauthorised equipment (e.g. USB drives or laptops) to any Highways England system or network.

6. Physical Security

You must take care regarding physical security of equipment, especially portable equipment such as laptops, tablets or portable memory devices.

You must not leave terminals, workstations, laptops and PCs unsecured once logged in past security systems (e.g. after entering an account name and password). Always lock the screen if you need to leave a system unattended.

If using a laptop or portable memory device to store Highways England data, you must ensure that the device or laptop is encrypted and not left in vehicles overnight.

You must store any sensitive data such as digital keys or certificates in an encrypted form.

7. Computer Hygiene

You must never access or use any data or program from any removable media or where received by electronic means e.g. email attachment, until the media or attachment has been passed as safe to use by an anti-virus utility.

You must ensure that all devices used to access TTD systems have functioning and up to date anti-virus software installed and be running a fully configured local firewall.

You must not use personally-owned computer equipment to access TTD systems unless authorised by TTD.

8. What to do in the event of an Information Security Incident

If you see or are exposed to an Information Security incident or suspect that you have been exposed to an Information Security incident, e.g. lost laptop, virus infection and that incident affects or potentially affects TTD systems then you (or your project/organisation) must inform the Project Sponsor and the RMAS service desk of the incident as soon as reasonably possible. The RMAS security management team will forward a report to the TTD Information Security Team and perform an initial investigation of the issue.

You should also follow your own company's procedures regarding the reporting of Information Security incidents in addition to the above reports.

The RMAS service desk can be contacted at: support@simulation-systems.co.uk