HATMS - Information Security

Information Security

Information Security is critical to ensuring the protection of the Highways Agency's (HA) business assets and processes.

An important part of minimising the risk to HA systems is to ensure that users of HA systems understand the behaviour expected of them.

This procedure applies to all persons accessing Highways Agency Traffic Technology Division systems or services where the systems or services are managed or provided through HATMS.

This advice is general in nature. Most companies will have in place specific policies and procedures to deal with the management of Information Security and you should follow those polices in addition to the requirements of this document.

Access and accounts

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

- Accounts and passwords should not be shared.
- Passwords should never be divulged to anyone else.
- Passwords should:
    - be changed regularly;
    - 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.

For accounts managed through the HATMS Common Sign-on facility, password complexity and length will be automatically enforced.

Accounts will only be issued to individuals who have been approved by the Highways Agency and authorised to access specified HATMS systems.

When your account is issued, you will be told for which systems the account is valid. Under no circumstances should you use your account to access a system or service for which the account has not been authorised.

Data Security and Confidentiality

In general, the business-related data obtained from HATMS is not confidential in nature. Data from systems that are not part of HATMS but are accessed via HATMS may be confidential in nature. Those projects responsible for non-HATMS data will have defined the confidentiality of that data.

Data obtained from HATMS will be Crown Copyright and so should not be distributed to other persons or organisations without prior written authorisation from the Highways Agency.

Network and Service Monitoring

The Highways Agency and the HATMS project monitor and may record activity on managed networks and services for lawful purposes. No notification will be given of any such monitoring or recording.

External Connections

You must not connect unauthorised equipment (e.g. USB drives or laptops) to any HATMS system or network without explicit and prior permission from the Highways Agency.

Physical Security

You should take particular care regarding physical security of equipment, especially portable equipment.

Terminals, workstations, laptops and PCs should not be left unsecured once logged in past security systems (e.g. after entering an account name and password).

Portable memory devices and laptops used to store Highways Agency data should use an encrypted file system.

Systems or devices used to store sensitive data such as digital keys and certificates must use an encrypting file system.

Computer Hygiene

Never execute any program or application macro from any storage medium or where received by electronic means, until the program has been passed as safe to use by an anti-virus utility. Similar caution should be applied to media and electronic sources transferred from within your organisation unless you are satisfied that such material has already been adequately checked.
All systems used to access HATMS or other Highways Agency systems must have functioning and up to date anti-virus software installed.
Computer equipment connected to an “always on” type Internet facility (e.g. fixed or mobile broadband) should have a local firewall running on it.

What to do if you suspect that your PC or system has been infected by a virus

Disconnect from the network and prevent the use of computer until decontaminated.
Inform your company's IT department and follow any procedures that they have in place to deal with such incidents.

Secure any media that may have been contaminated and prevent its use until checked (and decontaminated if necessary).
Inform all parties that have recently used your computer or received media or files generated on your computer of the possibility of infection.

Inform the HATMS Help Desk and the Highways Agency.

Point of contact in the event of an Information Security incident

If you suffer an Information Security incident, e.g. lost laptop, virus infection and that incident affects HATMS or HATMS-related systems then it is important that you (or your project/organisation) inform the HATMS Help Desk of the incident.

You should also follow your own company's procedures regarding the reporting of Information Security incidents.

HATMS Helpdesk Details

Mott MacDonald Ltd.

1 Atlantic Quay

Broomielaw

Glasgow

G2 8JB

T: +44(0)141 222 4666

F: +44(0)141 222 4667

HATMS_Helpdesk@mottmac.com