Vehicle & Operator Services Agency

Information Security Policy

Version 2.0

Document control

Document Information

Document Author:	David Williams
Next review date:	1st April 2014 and at least annually therefater
Retention period:	Refer to VOSA Records Manager

Version history

Tool Used	**Microsoft Word 2003**		
Version	**Date**	**Changed by**	**Comments**
1.0	23/01/13	David Williams	For TUS Consultation
2.0	10/04/13	David Williams	Final after TUS consultation

Issue control

Owner and approver:	Andrew White	
Role:	Chief Information Officer / VOSA SIRO	
Signature:		**Date:**

Changes since last version

Update to Para 4.4 to reflect organisational change

Distribution List

Contents Page

1. Introduction

1.1 This policy is intended to ensure that all data stored, sent or processed by VOSA (or by authorised delivery partners and third parties on behalf of VOSA) is protected with a proportionate level of security from events which may compromise its confidentiality, integrity or availability.

1.2 At all times, VOSA will seek compliance with the requirements set out in HMG Information Assurance (IA) Standards 1 to 7 and HMG Security Policy Framework, together with Good Practice Guides published periodically by Central Electronics Security Group (CESG) and this Policy endorses that aim.

1.3 This Policy will be maintained, reviewed and updated by the VOSA Data Security Manager. This review will take place at least annually. Any proposed changes to the policy will be subject to formal consultation with the VOSA TUS.

1.4 VOSA is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of VOSA, who may be held personally accountable for any breaches of information security for which they may be held responsible. VOSA will ensure that staff receive necessary training in accordance with Cabinet office requirements, including refresher training on an annual basis.

1.5 In support of this Policy, VOSA will maintain a Document Set to fulfil a number of requirements of the HMG Security Policy Framework, the Information Assurance Maturity Model and the Information Assurance Assessment Framework.

2. Purpose of this policy

2.1 This Policy describes at a high level VOSA's approach to securing data and developing a culture throughout the organisation which is aware of security issues, as well as being compliant with legislative and HMG Information Security requirements.

2.2 This Policy supports VOSA's Information Assurance Strategy which informs VOSA's delivery plans to comply with the HMG Security Policy Framework and with HMG Information Assurance Standards, and build processes which support continuous improvement of our information assurance measures. The VOSA Information Assurance Strategy supports the Cabinet Office National IA Strategy and the DfT IA Strategy.

2.3 Information Security forms a part of the wider Information Assurance function within VOSA. Information Assurance (IA) is defined by the HMG Security Policy Framework as "the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users". VOSA works to gain this assurance through an ongoing range of IA activities, including the measures and methods described within this policy.

2.4 Therefore, the objectives of the VOSA Information Security Policy are to assist VOSA in ensuring the following in relation to its information:

- **Confidentiality** - Access to data will be confined to those with appropriate authority.
- **Integrity** – Information will be complete and accurate. All systems, assets and networks will operate correctly, according to specification.
- **Availability** - Information will be available and delivered to the right person, at the time when it is needed.

2.5 VOSA will aim to achieve the above objectives by:

- Ensuring that all persons and organisations handling VOSA information are aware of and comply with the relevant legislation as described in this and other policies, all of which are aimed at protecting the information assets under the control of the organisation.
- Describing the principals of security and explaining how they will be implemented in the organisation and by organisations handling information on behalf of VOSA.
- Introducing a consistent approach to security, ensuring that all persons and organisations handling VOSA information fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Working with delivery partners to ensure that accurate relevant information is available when required to support VOSA's activities.

2.6 This policy supports the ATOS Security Plan for VOSA.

3. Scope

3.1 This policy applies to all information, information systems, networks, applications, locations and users of VOSA or supplied under contract to it. 'Information' includes both personal and non-personal information.

3.2 This policy applies to all areas of VOSA, including:

3.2.1 All VOSA employees (permanent, fixed term, full-time and part-time) whether working at VOSA premises or performing remote working

3.2.2 All agency and contractual workers as above

3.2.3 All Delivery Partners and Third Party Supplier staff processing information on behalf of VOSA.

3.3 Where this policy states 'VOSA staff' or 'all staff' it should be read to include the entities above including staff working for Delivery Partners and Third Party Suppliers processing VOSA information.

4. Responsibilities for Information Security

4.1 All VOSA staff and any third parties who access VOSA sites, systems or information must act in accordance with this policy. It is the responsibility of all staff to:

- report potential or realised risks to VOSA information
- handle information securely and in accordance with the HMG Protective Marking System where applicable and to other relevant standards
- ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Failure to do so may result in disciplinary action.

4.2 VOSA's Chief Executive will fulfil the role of Accounting Officer (AO). The AO is responsible for approving and signing the Annual Statement of Internal Control, which is then supplied to the Cabinet Office. The AO has ultimate responsibility for ensuring that information risks are assessed and mitigated to a level which is acceptable in line with VOSA's stated risk appetite.

4.3 The management of information risk will be owned and represented at Board level by the Senior Information Risk Owner (SIRO). VOSA will ensure that the SIRO receives appropriate training for this role.

4.4 The VOSA Cryptocustodian, who is a member of VOSA's staff, will manage the VOSA account with CESG relating to cryptographic material supplied by that body and provides advice relating to cryptographic material in accordance with HMG Information Assurance Standard 4 and any other relevant standards. CESG is part of Government Communications HQ (GCHQ).

4.5 The VOSA Data Security Manager will lead a team which will provide advice and guidance to VOSA on security issues. This team will also manage the accreditation and security testing schedule for VOSA systems. VOSA will ensure that the members of this team receive appropriate training for their roles.

4.6 The VOSA Data Security Manager will be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

4.7 The VOSA Data Security Manager will chair regular meetings of the Security Review Committee, which includes representatives from areas of VOSA business, together with representatives of Atos (for both the VOSA infrastructure & MOT Computerisation), where security matters can be raised and discussed.

4.8 The VOSA Data Security Manager will maintain, review and update the Information Security Policy at least annually. Any proposed changes to the policy will be subject to formal consultation with the VOSA TUS.

4.9 The VOSA Data Security Manager will keep the VOSA Senior Information Risk Owner, VOSA Business Delivery Board, VOSA Directing Board, VOSA Audit and Risk Committee and the DfT Departmental Security Officer informed of the information assurance status of the organisation by means of regular reports and presentations.

4.10 VOSA has nominated Information Asset Owners (IAOs) for specific Information Assets. These Assets are assessed as being of value to VOSA. The Assets may include personal information, non-personal information or both. Responsibilities of these IAOs are as described in HMG Information Assurance Standard 6. VOSA will ensure that IAOs receive appropriate training for their role.

4.11 The Director with responsibility for Estates, Facilities and Finance holds overall responsibility for physical security measures, supported by the VOSA Data Security Manager and the VOSA Health and Safety Manager.

4.12 All Line Managers are responsible for ensuring that:

- VOSA equipment is returned by staff prior to changing role or leaving VOSA
- Access to Information Assets is revoked on the termination of their employment, contract or agreement
- The physical security of the environments under their direct control where information is processed or stored is maintained appropriately, and deficiencies are reported accordingly.

4.13 Third parties and Delivery Partners are responsible for supplying evidence of their compliance with HMG Security Standards and with this policy. Contracts with external contractors that allow access to the organisation's information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies. All contracts where information is handled on behalf of VOSA will be in accordance with latest Office of Government Commerce requirements relating to data handling, data protection and information security.

5. Outsourcing and offshoring

5.1 Proposals for outsourcing the processing or storage of VOSA information or for off-shoring of such functions must be notified to the VOSA Data Security Manager and the VOSA Senior Information Risk Owner, and must not take place unless fully authorised by DfT. Such proposals will be considered in line with relevant HMG Policy, including CESG Good Practice Guide 6.

6. Asset classification and control

6.1 VOSA will promote compliance with the HMG Protective Marking System. Guidance on the use of the Protective Marking System and the handling of protectively marked data will be available to staff to ensure that information is protected by appropriate controls and technical measures throughout its lifecycle, including creation, storage, transmission and destruction.

6.2 Information will be classified in accordance with the HMG Protective Marking Scheme. Classifications include:

- Not Protectively Marked or Unclassified
- Protect
- Restricted
- Confidential
- Secret
- Top Secret

together with relevant descriptors.

6.3 Relevant Information Asset Owners will use Business Impact Levels to assess the risk of compromise to confidentiality, integrity and availability of their Information Asset.

6.4 Security Aspects Letters will be completed for major IT system assets. These will define the classification of major IT assets including datasets and will define the security requirements applicable to those assets.

7. Information Security Awareness Culture and Training

7.1 Information security awareness training will be included in the staff induction process and repeated on at least an annual basis. This may vary on occasion from a written reminder to all staff of their responsibilities relating to Information security, to formal training provided via e-learning .Where resources permit, face- to face delivery will be considered where appropriate General advice and training will be available to all staff, and more bespoke training will be given to nominated roles. The VOSA Information Security Team provides a resource for all staff in relation to advice on Information Security matters.

7.2 VOSA will ensure that an ongoing programme is maintained in order to ensure that staff awareness is refreshed and updated as necessary. Internal communications methods will be used for this purpose.

7.3 The Information Security team will monitor ‘best practice’ methods through attendance at seminars and conferences and, where it is possible and of benefit to VOSA, seek to implement those practices.

7.4 The effectiveness of VOSA’s security policies, practices and controls will be monitored by the Security Review Committee and the Audit and Risk Committee, and through periodic compliance audits (e.g. Security Policy Framework and Information Assurance Maturity Model). Results of these reviews will be used to determine where efforts should be concentrated.

7.5 VOSA will use tools such as periodic staff surveys to measure and monitor its security culture and will use the results of this process to inform future awareness programmes.

7.6 This Policy supports the measures outlined in the VOSA IA Cultural Change Plan.

8. Personnel Security

8.1 Staff security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. In line with HMG Policy on Personnel Security, all staff must be checked to at least Baseline Personnel Security Standard (BPSS). This is a civil –service wide requirement.

8.2 Information security expectations of staff will be included within appropriate job definitions.

8.3 Staff will be vetted (Basic Personnel Security Standard, Counter-Terrorism Check, Security Clearance or Developed Vetting) commensurate with the information they will be handling and the level of access they will have in line with the VOSA Policy on Vetting (see VOSAnet Information and Technology home page) and HMG Policy on Personnel Security (see VOSAnet Information Security resource section).

8.4 Vetting (including background checking and identity checking) of VOSA staff to BPSS standard is the responsibility of VOSA Human Resources Team via Departmental Resourcing Group. Some posts will require vetting above BPSS standard and applicants will be made aware if this is the case. All requests for vetting or clearance above BPSS (e.g. CTC, SC) will be referred to the VOSA Information Security Team, who will co-ordinate such applications in accordance with relevant VOSA Policy.

9. Access Controls

9.1 Access to information will be restricted to authorised users who have a bona-fide business need to access the information. The ‘need to know’ rule must apply at all times. Requests for access to information assets must be referred to and approved by the relevant Information Asset Owner for that asset.

9.2 Access to computer facilities will be restricted to authorised users who have business need to use the facilities. Authentication including use of passwords and other methods will be carried out in accordance with Information Assurance Standard no.7.

9.3 Access to data, system utilities and program source libraries will be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will depend on the availability of a licence from the supplier.

9.4 Where the need to access information ceases due to a change in role, misuse or termination of employment or contract, those access rights will be withdrawn. It is the responsibility of the outgoing line manager of the member of staff to ensure this takes place.

9.5 An audit trail of system access and data use by staff will be maintained and reviewed on a regular basis by relevant Information Asset Owners. VOSA has in place processes to audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the relevant legislation and CESG guidance.

10. Physical Security

10.1 Due to the geographically disperse and varied nature of the VOSA estate, carrying out an assessment of the security of every VOSA building using HMG methodology would involve expense which is disproportionate to the risk to VOSA information. Instead, VOSA will carry out physical assessments intended to cover a representative sample of the estate. Dependent on resources, VOSA will carry out this assessment at least once every three years.

10.2 The above assessment of physical security will be carried out via an Internal Audit review, reporting to the VOSA Audit and Risk Committee.

10.3 The physical security of Delivery Partners and Third Party suppliers will be assessed in line with RMADS procedures, or independently where this is not appropriate.

10.3 All staff have a responsibility to report matters which could undermine the physical security of the VOSA estate.

10.4 All staff have a responsibility to ensure that they do everything that can reasonably be expected of them in ensuring that, in order to minimise loss of, or damage to, all assets, equipment will be physically protected from threats and environmental hazards.

11. Contract Management Requirements

11.1 The Office of Government Commerce (OGC) model security contract clauses will be embedded as appropriate within all new contracts which use Information Technology systems to store or process protectively marked VOSA information.

11.2 Procurement or letting processes will ensure that any necessary Confidentiality or Non-Disclosure provisions are included in contracts with third parties.

11.3 VOSA will fulfil the requirements of any mandated Code of Connection (CoCo) – and will provide assurance of compliance on at least an annual basis.

12. Information Risk Assessment and Management

12.1 The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence. HMG Information Security Standards 1 and 2 will be used for this purpose, along with HMG Business Impact Level Tables.

12.2 Once identified, information security risks will be managed on a formal basis by the VOSA Data Security Manager. The risks will be recorded within a baseline risk register and action plans will be put in place to effectively manage those risks. The risk register and all associated actions will be reviewed at regular intervals. Any implemented information security arrangements will also be a regularly reviewed feature of VOSA's risk management programme. These reviews will help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

12.3 VOSA will conduct annual security accreditation (including a technical risk assessment using HMG IA Standard 1) for all 'in scope' IT systems. Systems are deemed to be in scope or out of scope for the year's annual security testing and accreditation schedule through discussion with the Departmental Security Officer (DSO), who is the Department for Transport's Accreditation Authority. This results in a risk based decision on the level of testing and accreditation required.

12.4 New systems will be assessed as soon as possible to determine whether they currently (or will, once 'live') fall in scope and therefore require testing and/or accreditation. For this purpose, it is essential that the VOSA Information Security Team are involved at an early stage in project planning to ensure that projects and programmes are not delayed by security requirements at later stages of development.

12.5 A technical risk assessment is also performed when there are significant changes to existing 'in scope' IT systems in operation (for example significant changes in functionality, user base or threat).

12.6 Assessment and risk decisions are recorded in the Risk Management and Accreditation Document Set (RMADS), using HMG IA Standard 2 – Risk Management and Accreditation of Information Systems. The RMADS is then submitted to the Departmental Security Officer for approval. The DSO will assess the security of the system, along with its compliance to HMG IA Standards, and will award accreditation if the level of residual risk and use of security controls are acceptable.

12.7 All systems storing or processing information relating to 100,000 or more identifiable individuals will be subject to a penetration test. This is in line with HMG IA Standard 6 – Protecting Personal Data and Managing Information Risk.

12.8 VOSA will seek to reduce the risk posed by technical faults or vulnerabilities identified by technical risk assessments, by working with the supplier to provide adequate mitigation. In the case of systems which are in scope for accreditation, details of the mitigation of these risks will be provided to the DSO along with test results part of the accreditation process. If vulnerabilities are identified with systems which are not in scope for accreditation, the Information Security Manager will provide advice to the SIRO and the relevant Information Asset Owner, so that the level of residual risk can be assessed and either accepted or be subject to further mitigation work.

12.9 In order to provide suitably proportionate methods of handling information, Impact assessments are carried out or reviewed on a quarterly basis by designated Information Asset Owners. These assessments use the HMG Business Impact Levels to assess the risk to VOSA of the compromise to confidentiality, integrity and availability of the information.

12.10 New systems will be subject to Privacy Impact Assessments as required.

12.11 Systems will be supported by Security Operating Procedures as appropriate.

13. Communications and Operations Management

13.1 Computer and Network Procedures

13.1.1 Management of computers and networks will be controlled through standard documented procedures.

13.1.2 Where a Security Operating Procedure is in existence for a system, process or asset, any use must be in accordance with the relevant Security Operating Procedure. Users breaching this requirement may be subject to disciplinary action.

13.1.3 Use of VOSA ICT systems must be in accordance with the current ICT Acceptable Use Policy.

13.1.4 Mobile telephones, with the exception of VOSA issued Blackberry devices must not be used to connect to the VOSA e-mail service.

13.1.5 Any remote workers must comply with VOSA's remote working policy. The same rules and standards for use of VOSA telephones, computers, internet access and email systems apply to remote working as when in the office. Users must comply with VOSA policies and Security Operating Procedures (SyOps) relating to the use of specific items. These policies and SyOps will be published on the VOSA Intranet in the 'Information and Technology' and 'Information Security' sections of (VOSAnet).

13.1.6 It is the personal responsibility of all users to ensure that physical security of all devices is assured at all times, and any losses must be reported without delay.

13.1.7 All Blackberry remote access solutions must comply with current HMG Security standards including settings.

13.1.8 All laptops holding VOSA information must have full disk encryption that complies with HMG standards. Encryption will be deployed as appropriate in accordance with VOSA and HMG policy.

13.1.9 Only official equipment issued by VOSA may be used to store, process or transmit VOSA information. Personal equipment such as home computers must not be used, unless specific approval has been given by the VOSA Data Security Manager.

13.1.10 VOSA IT assets (including but not limited to laptops, Blackberrys and any other form of Personal Electronic Device) may not be taken out of the UK, unless express approval has been received from the VOSA Crypto Custodian. (There is no requirement to seek such approval in the case of VOSA-issued mobile telephones).

13.1.11 VOSA will provide updates and briefings to staff in order to create and support a culture which values and protects VOSA information.

13.2 Use of Removable Media

13.2.1 Removable media of all types must only be used in accordance with the Department for Transport Removable Media Policy, unless specific approval has been granted by the Department for Transport Senior Information Risk Owner.

13.2.2 USB Memory devices must only be used if they have been issued by VOSA Information Security Team and are encrypted to a minimum of FIPS140-2. No information with a Business Impact Level greater than IL2 may be held on such a device. No personal devices are permitted.

13.3 Technical defence measures

13.3.1 VOSA will use software countermeasures and management procedures to protect itself against the threat of malicious software.

13.3.2 All VOSA ICT systems must be protected by adequate antivirus and anti-malware systems to protect against these threats, and these must be kept fully updated.

13.3.3 Users will not install software on the organisation's property without permission from the VOSA Service Manager. Users breaching this requirement may be subject to disciplinary action.

13.3.4 All VOSA ICT Systems must be kept patched with the latest security patches. A period of User Acceptance Testing may be required before deployment, in order to prevent unforeseen effects on systems. .

13.3.5 All VOSA ICT systems must be maintained in line with mitigations recommended in GOVCERT alerts, or a risk based decision made and documented if any suggested mitigations cannot be applied.

13.3.6 All VOSA ICT Systems must be locked down in accordance with current VOSA and HMG requirements. VOSA will pursue compliance with all HMG Information Assurance Standards relevant to this policy and the Security Policy Framework

13.3.7 Perimeter defence measures will be deployed to protect VOSA ICT Systems in accordance with contract and Service Level Agreements.

13.3.8 A backup regime of VOSA ICT systems will be carried out in line with contracts and Service Level Agreements.

13.3.9 VOSA will pursue and maintain compliance with commercial security standards which are applicable to its operations, such as the Payment Card Industry Data Security Standards (PCI-DSS).

13.4 Security events and weaknesses

13.4.1 All information security incidents and suspected weaknesses are to be reported to the VOSA Data Security Manager in accordance with VOSA policy.

13.4.2 All information security incidents will be further reported to VOSA SIRO and to DfT Security. Relevant incidents will also be reported to national bodies (CINRAS, GOVCERT, Cabinet Office) as applicable.

13.4.3 All information security incidents will be investigated to establish their cause and impacts with a view to avoiding future similar events. Incidents will be discussed at the Security Review Committee meetings.

13.4.4 Incidents requiring forensic investigation will be handled in accordance with VOSA Forensic Readiness policy and Forensic Readiness Plan.

13.4.5 Where vulnerabilities are apparent (e.g. following IT Health Checks) these will be reported to the VOSA Data Security Manager and risk treatment plans developed accordingly.

14. System Change Control and New Initiatives

14.1 Major changes to VOSA systems must be approved by the Change Committee and the Change Approval Board before deployment.

14.2 Non-Standard IT change requests are documented using the Change Request System and are all subject to approval by the Information Security Team.

14.3. Additional requests for individual access to IT systems must be approved by the relevant Information Asset Owner for the relevant system.

14.4 All new Projects and initiatives involving the processing of personal or protectively marked information must be notified to the VOSA Data Security Manager, so that assessments can be made of risk to privacy and security, and formal accreditation sought where applicable.

15. Intellectual Property Rights

15.1 All products used with VOSA ICT Systems must be properly licensed and approved by VOSA Head of ICT Service Management. Users must not install software on the organisation's property without permission from the VOSA Head of ICT Service Management. Users breaching this requirement may be subject to disciplinary action.

16. Business Continuity and Disaster Recovery Plans

16.1 VOSA and its major delivery partners will develop Business Continuity Plans for locations within VOSA control where protectively marked information (including cryptographic items) is held.

16.2 VOSA will develop Disaster Recovery Plans for mission critical information, applications, systems and networks.

16.3 Business Continuity and Disaster Recovery plans will be tested, with 'lessons learned' sought and included in planning.

17. Information Sharing

17.1 Any sharing of information will only be carried out in accordance with DfT Data Sharing Policy. In all instances the sharing will only take place where:

- It is permitted by law
- It is only carried out in accordance with legislation (e.g. Data Protection Act 1998 principles)
- It has been approved by VOSA Information Security, VOSA SIRO (and DfT)
- It is subject to sharing agreements by all parties involved
- Adequate security is assured by all parties involved

17.2 All new requests to share VOSA data, or to share the data of other organisations, will be notified to the VOSA Data Security Manager and must be subject of an agreed Memorandum of Understanding before commencement of sharing.

17.3 Where arrangements already exist which are key to VOSA operations, they will be reviewed and subjected retrospectively to an agreed Memorandum of Understanding.

17.4 VOSA will operate with due compliance to the requirements of all relevant legislation, such as the Data Protection Act 1998 and the Computer Misuse Act 1990

18. Delivery Partners and Major Service Providers

18.1 Delivery Partners and Major Service Providers of VOSA will be expected to comply with the requirements of this Policy when they are handling VOSA information.

18.2 Any breaches of this Policy by Delivery Partners or Major Service Providers must be notified to the VOSA Information Security Manager without delay.

18.3 Any incident involving loss or potential loss of VOSA information by Delivery Partners or Major Service Providers must be notified to the VOSA Information Security Manager without delay.

18.4 VOSA reserves the right to carry out audits on the levels of compliance with this Policy by Delivery Partners and Major Service Providers, including audit to ISO 27001 standards where appropriate.

18.5 This policy supports the ATOS Security Plan for VOSA.