Greater London Authority
Information Security Policy

1. Purpose

The purpose of the Information Security Policy (the "Policy") is to ensure that the Greater London Authority's (the "GLA's") Information (as defined below) is kept safe and secure and that appropriate procedures and guidance are in place to:

- Protect its integrity, availability and confidentiality;
- Minimise the potential consequences of Information security breaches by preventing their occurrence in the first instance or, where necessary, containing and reducing their impact; and
- Ensure that personal data is afforded the protection required by the Data Protection Act 1998.

2. Scope

This Policy:

- applies to the whole of the GLA: the Mayor, Assembly Members and all staff including agency workers, secondees and consultants engaged to work with the GLA.
- covers all Information (as defined below) held by the GLA, and/or staff of the GLA and others who are engaged to work for the GLA.

3. Definitions

For the purposes of the Policy, "Information" is defined as any Information, data or records, irrespective of format, which are generated or used by the GLA in the carrying out of its functions. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.

4. Policy Statement

The Information is the property of the GLA and a vital asset to the organisation. The GLA recognises the importance of this Information and will take all necessary measures to ensure that it is secure from loss, unauthorised or unlawful processing, damage or destruction. In doing this, the GLA will use ISO 27001:2005 or equivalent (the International Standard on Information Security) as a benchmark against which to measure its progress. The GLA is committed to ensuring that its policies comply with all relevant legislation such as the Data Protection Act 1998.

Specifically, the GLA is committed to:

- Taking responsibility for Information security matters at senior management level, including a regular forum – the Governance Steering Group ("the GSG") where Information security issues can be discussed and new initiatives authorised.

- Producing and communicating guidance and procedure documents covering all relevant areas of Information security and ensuring that these procedures are complied with.
- Implementing systems, both manual and electronic, to ensure that Information is kept as securely as possible.
- Reviewing the Policy and all associated material every two years.

5. Roles and Responsibilities

Senior management will oversee and monitor Information security issues within the GLA as part of the GSG which meets every six weeks. The GSG is chaired by the Director of Resources and its members include the Head of Paid Service and the Head of Committee & Member Services/Monitoring Officer.

The Head of IT and the Information Governance Manager also attend this group and will manage the implementation of the Policy by producing and reviewing procedures and guidance for the GLA as required.

The Mayor, Assembly Members and all staff of the GLA, including agency workers, secondees and consultants engaged to work with the GLA, are responsible for implementing Information security good practice on a day to day basis through compliance with the Policy and associated guidance and procedures.

6. Methods of implementation

Policies and procedures will be used to support the Policy, including:

- Business continuity plans and the emergency contact procedure
- The Code of Ethics and Standards for Staff, including the protocol on use of Information and Communications Technology (ICT) and Terms and Conditions of Employment, in particular:
    - Disciplinary procedure
    - Confidentiality provisions for staff
    - Termination of employment procedures
- Clear desk and clear screen guidance
- Guidance on Remote working
- Guidance on Data protection
- Guidance on Freedom of Information
- The staff induction process will include information on this
- Records management policy, including guidance and tools provided to support it
- Guidance on handling of Information security breaches
- Guidance on handling computer viruses and other attacks on the IT infrastructure
- Use and secure handling of equipment used to hold or access GLA Information, eg laptops, blackberries, etc

Each team that the GSG identifies as having a lead role or responsibility for Information security, will be required to review its relevant policies, procedures and working methods and report to the GSG. For example:

1. ICT
    - The IT infrastructure (including remote working infrastructure) will be reviewed on a regular basis to ensure that it is as secure as practicable..
    - Specification, procurement and authorisation for new Information systems will include security considerations..
    - Information held in electronic format will be backed up securely so that it can be restored as necessary.
    - All emails will automatically have GLA disclaimers added when sent.
    - Personal data will be processed lawfully and in line with the rights of data subjects; such data (and in particular sensitive data) will be protected from unauthorised access.

2. HR
    - Staff will be informed of their responsibilities for the security of the GLA's Information by relevant changes to terms and conditions, policies and procedures. Policies and procedures will be updated to cover inappropriate disclosure and misuse of Information.
    - Arrangements for engaging temporary staff will be reviewed to ensure that all policies and procedures on Information security apply to temporary staff
    - Staff and others will be informed of any changes to procedures that may impact on them.

3. FM
    - Arrangements for allocation and termination of access passes will be reviewed on a regular basis.
    - Adequate facilities for the secure storage of Information held in material form will be provided.

4. Information Governance
    - Guidance on Information and records management will be maintained and developed, including guidance about ensuring that computers are locked when unattended and papers filed as securely as required, as well as disposing securely of Information in whatever form.
    - Dealing with Data Protection Act issues (risks, complaints, breaches), including ensuring awareness and maintaining and updating guidance as required.
    - Guidance on utilising Information Sharing Protocols to safeguard Information that is shared with third parties will be created and maintained.

7. Review of this Policy

This Policy will be reviewed every two years to ensure that it is up to date. The review will be carried out by the GSG.

Appendix – Legislation and Standards relevant to Information Security

Legislation and regulations

- Data Protection Act 1998
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Greater London Authority Acts 1999 and 2007
- Human Rights Act 1998
- Limitation Act 1980

Standards and Codes of Practice

- BS ISO 15489 Information and documentation – Records Management
- BSI BIP 0008 Code of practice for legal admissibility and evidential weight of Information stored on electronic document management systems
- BSI BIPD 0010 Principles of good practice for Information management
- BS ISO 27001:2005 – updated in October 2007 - International Standard on Information Security
- BS 7799 Code of practice for Information security management
- The National Archives' Requirements for Electronic Records Management Systems
- The Lord Chancellor's Code of Practice on the Management of Records Issued under section 46 of the Freedom of Information Act 2000