LGfL Information Security & Information Management Policy

1. Introduction

The purpose of this document is to set out the Service Provider's requirement of the Service Aggregator in having adequate and appropriate information security standards and data sharing arrangements in place through their policies, procedures and working practices.

2. Policies and Procedures

The Service Aggregator shall have and shall ensure that the Service User's have information security policies and data sharing arrangements in place which are based on industry best practice and which address, as a minimum, the following statutes, or their successors:

- Children Act 2004
- Data Protection Act 1998
- Computer Misuse Act 1990 / Police and Justice Act 2006 (Sections 35 – 38)
- Freedom of Information Act 2000
- Human Rights Act 1998
- Employment Acts
- Relevant EU Directives on Data Protection

As such the policies should be drawn upon relevant best practices including:-

3.1.1. "Information Security Management Systems – Requirements" (ISO/IEC 27001); and

3.1.2. "Information Security Code of Practice for Information Security Management" (ISO/IEC 27002).

And we expect the policy to address the following areas:

- Risk assessment and mitigation activities
- Organisation and governance of information security
- Provision for appropriate management of information and physical assets
- Use of privacy impact assessments
- Human resources impact including:-
  - Job and person specifications
  - Staff awareness
  - Professional development
- Communications and operations impact including:-
  - Operational procedures and responsibilities
  - Systems planning and acceptance
  - Protection against malicious software
  - Back-up procedures
  - Network and infrastructure management
  - Media handling and sensitivity
  - Exchanges of information and software
  - Internet and e-mail
- Physical and environmental security impact including:-
  - Secure locations
  - Equipment security

    - General controls
- Access controls including:-
    - Business requirement for access control
    - User access management
    - User responsibilities
    - Network access control
    - Operating system access control
    - Application access control
    - Monitoring system access and use
    - Mobile computing and remote users
    - Federated arrangements and external interfaces
- Information systems acquisition, development and maintenance including:-
    - Security requirements of Systems
    - Security in Applications Systems
    - Cryptographic controls
    - Security of systems files
    - Security in development and support processes
- Information security incident management and learning
- Data sharing agreements including:-
    - Information Sharing Protocols
    - Appropriate transportation of sensitive information
- Business continuity management
    - Aspects for business continuity management
    - Disaster Recovery Planning
- Compliance activities including:-
    - Compliance with legal requirements
    - Reviews of security policy and technical compliance
    - Review of organisational awareness and skills
    - System audit considerations

3.2. The Service Aggregator shall immediately inform the Service Provider in writing if it becomes aware of, or suspects any failure to comply with the requirements in this schedule and ensure that any risks are mitigated. The Service Aggregator shall provide evidence to the Service Provider that the breach has been rectified within five (5) Business Days of a request by the Service Provider.

3.3. The Service Aggregator shall cooperate and coordinate with the Service Provider or its nominated agents on security matters.

3.4. The Service Aggregator shall ensure that all relevant information (including records and data) produced or created in the course of providing the Services shall be evidentially admissible (and, where relevant, capable of certification) in accordance with the requirements of the law in relation to criminal proceedings, and shall lend the Service Provider's assistance in any such criminal proceedings as the Service Provider may reasonably require from time to time.

3.5. At the direction of the Service Provider, audit trail and all relevant information (including records and data) produced or created in the course of providing the Services necessary to support live investigations and prosecutions shall be retained by the Service Aggregator for the duration of the investigation and prosecution irrespective of the normal retention period of that information.

LONDON
GRID FOR LEARNING