NIGB

System Level Security Policy (SLSP)

Introduction:

The development, implementation and management of a System Level Security Policy (SLSP) will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

An effective SLSP will therefore contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise) of patient identifiable / sensitive data

Current encryption guidance for NHS organisations can be found in "Guidelines on use of encryption to protect person identifiable and sensitive information", and we would expect any electronic solution for the handling of patient identifiable / sensitive data to comply with this guidance as a minimum.

Where the system is available to multiple organisations, the SLSP must establish the necessary common policy, security parameters and operational framework for that system's expected operation including any functional limitations or data constraints applicable to one or more bodies.

The SLSP is a core component of an accreditation documentation set for those organisations that undertake formal accreditation processes for their information assets.

System Details

- The System shall be known as the *BRAIN UK* Database
- The System's responsible owner shall be Division of Clinical Neurosciences, Clinical and Experimental Sciences, Faculty of Medicine, University of Southampton ("the University")
- The System's Caldicott Guardian or Data Controller shall be Dr. Clare Mitchell (supervisor Professor James A. R. Nicoll).

System Security

- The University of Southampton is currently reviewing its corporate Information Security policy with the intention of aligning working practices to the UCISA Information Security Toolkit which is based upon ISO27001:2005, using a subset of the controls specified in ISO27002:2005. Many policies and processes are already in alignment or are newly implemented within the spirit of the updated ISO27001:2013, although formal capability matching has not yet taken place.

A number of applicable policies are in place:

Regulations for the use of Computers and Voice and Data Communications Networks

Electronic Communications Policy

Regulations for the Use of iSolutions Resources

1. The system's responsible Security Manager shall be Dr. Clare Mitchell.

2. The Security Manager's duties shall include:

    - Identification of all appropriate statutory, regulatory and best practice requirements relating to Information Security
    - Identification and assessment of system related risks in liaison with the iSolutions Head of Information Security
    - Implementation of appropriate security controls to satisfactorily address identified risks.
    - Accreditation of security measures, including external validation as required, with the assistance of the iSolutions Head of Information Security
    - Communication of security responsibilities to other parties using the system
    - Maintenance of the risk register relating to the system, with the assistance of the iSolutions Head of Information Security

3. The system shall incorporate the following security controls (with reference to the guiding elements of ISO27002:2013 code of practice where appropriate; this does not however imply compliance with all aspects of ISO27002:2013):

    - Physical
        - Limited room access (via keypad) (ISO27002:2013 11.1.2)
        - Card activated magnetic locks at both entrances to adjoining corridor (ISO27002:2013 11.1.2)
    - Access control
        - Network logins ensure access by authorised staff: project staff, project supervisor and authorised iSolutions staff under supervision (ISO27002:2013 9.2.3)
        - Enforced regular robust password changes 9ISO27002:2013 9.4.3)
        - Review of user access rights at regular intervals (ISO27002:2012 9.2.5)
    - Cryptography
        - Full disk encryption of all PCs accessing BRAIN UK data using MS Bitlocker as per iSolutions policy (ISO27002:2013 10.1.1)
        - Central recovery keys for MS Bitlocker with restricted administrator access (ISO27002:2013 10.1.1)
    - Network
        - Connectivity to LAN network to access centrally-stored BRAIN UK data
        - PC Windows Firewall enabled as per iSolutions policy (ISO27002:2013 13.1.3)
        - Symantec Endpoint Protection anti-virus/malware enabled as per iSolutions policy (ISO27002:2013 12.2.1)
    - Storage and backups
        - BRAIN UK data stored on networked SAN storage dedicated to University research data in secure University data centre; access restricted by AD permissions to authorised staff and minimal set of senior trusted administrators. (ISO27002:2013 9.4.1)
        - Access permissions shall be reviewed on a regular basis and following exceptional events such as termination of employment (ISO27002:2013 9.2.5)
        - Backups maintained via daily snapshot for minimum of 90 days, with offsite mirror for business continuity reasons (ISO27002:2013 12.3.1 c, d, f)

    - Secure physical destruction of unwanted magnetic, optical and flash media (ISO27002:2013 8.3.2 and 11.2.7)
- Other (including authentication or certification arrangements, security testing, and audit)
    - Reviews of the SLSP will be initiated by the Security Manager and the iSolutions Head of Information Security on a regular basis. (ISO27002:2013 18.2.1)

System Management

4. The System shall be implemented by iSolutions (underlying operating system and database software) with the application software being developed and maintained by Dr. Clare Mitchell, with technical support provided by iSolutions.

5. The system will only be accessed by *BRAIN UK* Data Co-Ordinators on a routine basis and will be made available to the *BRAIN UK* Director (Professor James A. R. Nicoll) and his deputy (Dr David Hilton) upon request**.**

System Design

6. The System shall be accessible from any staff University PC with permitted access control. This will be accomplished by the provision of a folder on University research storage, housed within a secure University data centre, with access permissions set and verified to permit only those with authorised user access.

   Backups of the data will be taken automatically via functionality inherent in the storage, providing a minimum of 90 days snapshots of the data for recovery purposes, and mirrored to an offsite secure University data centre for business continuity purposes.

   (Current configuration provides snapshots every 2 hours, retained for one month, and offsite replication every 6 hours, retained for 3 months)

   Client access will be via Windows based PCs provided by iSolutions, with security measures inherent in the design of this platform: Minimised user rights (no administrative rights), Firewall and anti-virus/anti-malware software provided, regular and timely security patching, central access logging.

   By storing the data on networked storage, risk of theft or loss of data on the client PCs is minimised. Further encryption and securing of the client PCs minimises further risk of loss of data via data remnants, swapfile contamination and orphaned temporary files.

Operational Processes

7. Patient identifiable/sensitive data will be rendered linked-anonymised (pseudonymised) by the removal of patient identifiable information by the information provider prior to the inclusion in the BRAIN UK database.

   The resulting linked-anonymised dataset, while sensitive, cannot be used for identifying a patient. It will, therefore will be disseminated from the originating site to the University of Southampton by using an encrypted Zip file (AES-256 encryption; many Zip programs offer this functionality) and the use of the University's 'Dropof'f service (https://dropoff.soton.ac.uk) for secure transmission of the file. The password for the zip file shall be communicated via another medium; telephone, post or email to an alternative email account used for the 'Dropoff' process.

   Should linked-anonymised data require physical transport for any reason, an encrypted USB drive will be used that conforms to NHS-approved standards (FIPS-140-2; 3-DES or AES, to

256-bit strength. Kingston Technology DataTraveler Locker 4GB 256-SHA is a typical approved device).

The BRAIN UK database will not store any patient identifiable information either electronically or in a written or printed format.

8. Data will be stored electronically on a networked storage system dedicated to University research data.

9. Client PC systems will be secured as detailed in System Design.

10. The System's authorised users shall be *BRAIN UK* Data Co-Ordinators and identified members of the iSolutions Serviceline Response Team. Named iSolutions users are provided in Appendix A.

11. When the system or its data has completed its purpose or is otherwise no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data:

    - Network storage will be deleted; following this deletion, data will remain in backup systems for 90+ days until expired.
    - Keys relating to encrypted storage media will be intentionally destroyed.
    - Non-working media will be physically destroyed.
    - Optical media will be physically destroyed.

System Audit

12. An internal review of the system and associated risk register will be undertaken on an annual basis in conjunction with the iSolutions Head of Information Security, in the spirit of ISO27001:2013 9.2

    Where unacceptable risks are identified, improvements shall be undertaken. Continual improvement activities will be undertaken to ensure the continued effectiveness of security controls on the system.

System Protection

- Backups of the data will be taken automatically via functionality inherent in the networked storage, providing a minimum of 90 days snapshots of the data for recovery purposes, and mirrored to an offsite secure University data centre for business continuity purposes.

  (Current configuration provides snapshots every 2 hours, retained for one month, and offsite replication every 6 hours, retained for 3 months)

- Overall business continuity is addressed via the University's and subordinately iSolutions' business continuity plan.

System Level Security Policy Ownership

19. This SLSP shall be the responsibility of Dr. Clare Mitchell**.**

20. This SLSP shall be made available to authorised users and relevant regulatory bodies (NIGB-ECC).

21. This SLSP shall be reviewed on an annual basis for its completeness and for relevant update.

Data Protection Registration

22. Please confirm that your organisation has Data Protection Registration to cover the purposes of analysis and for the classes of data requested.

    Data Protection Registration Number: Z6801020
    http://www.ico.gov.uk/ESDWebPages/search.asp?Registration=Z6801020

This register entry describes, in very general terms, the personal data being processed by:

UNIVERSITY OF SOUTHAMPTON

Nature of work - University

Description of processing

The following is a broad description of the way this organisation/data controller processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have received, check any privacy notices the organisation has provided or contact the organisation to ask about your personal circumstances.

Reasons/purposes for processing information

We process personal information to enable us to provide education and support services to our students and staff; advertising and promoting the university and the services we offer; publication of the university magazine and alumni relations, undertaking research and fundraising; managing our accounts and records and providing commercial activities to our clients. We also process personal information for the use of CCTV systems to monitor and collect visual images for the purposes of security and the prevention and detection of crime.

Type/classes of information processed

We process information relevant to the above reasons/purposes. This may include:

- personal details
- family details
- lifestyle and social circumstances
- education details and student records
- education and employment details
- financial details
- disciplinary and attendance records
- vetting checks;
- goods or services provided
- visual images, personal appearance and behaviour
- information held in order to publish university publications

We also process sensitive classes of information that may include:

- racial or ethnic origin
- trade union membership
- religious or other similar beliefs
- physical or mental health details
- sexual life
- offences and alleged offences
- criminal proceedings, outcomes and sentences

Who the information is processed about

We process personal information about:

- students
- employees, contracted personnel
- suppliers, professional advisers and consultants
- business contacts
- landlords, tenants
- complainants, enquirers
- donors and friends of the University
- authors, publishers and other creators
- persons who may be the subject of enquiry
- third parties participating in course work
- health, welfare and social organisations
- friends of the University
- individuals captured by CCTV images

Who the information may be shared with

We sometimes need to share the personal information we process with the individual themself and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- family, associates and representatives of the person whose personal data we are processing
- current, past or prospective employers
- healthcare, social and welfare organisations
- educators and examining bodies
- suppliers and service providers
- student union
- financial organisations
- debt collection and tracing agencies
- auditors
- police forces, security organisations
- courts and tribunals
- prison and probation services
- legal representatives
- local and central government
- consultants and professional advisers
- trade union and staff associations
- survey and research organisations
- press and the media
- voluntary and charitable organisations
- landlords

Transfers

It may sometimes be necessary to transfer personal information overseas. When this is needed information may be transferred to countries or territories around the world. Any transfers made will be in full compliance with all aspects of the data protection act.

Statement of exempt processing:

This data controller also processes personal data which is exempt from notification

Appendix A - List of current iSolutions staff authorised to interact with BRAIN UK data

Name	Role
Darren Hampton	Head of Information Security
Jake Dovey	Serviceline Response Team member
Mike Bromley	Serviceline Response Team member
Kevin May	Serviceline Response Team member
Paul Carrington	Systems Management member
Ambrose Neville	Systems Management member
Mark Watts	Systems Management member