  

**System Level Security Policy (SLSP)**

**International DSD REGISTRY**

# International DSD Registry

Details of the I-DSD Registry background are available in the SOP.

The System Level Security Policy (SLSP) for I-DSD Registry has been developed through a formal process of risk assessment by Prof Ahmed & Dr Watt documented in this document. It covers security and management procedures in place throughout for data collection, data handling, data storage, data analysis and data destruction for clinical projects involving the [IT](http://IT) Services e-Science at the University of Glasgow. It details the lines of accountability within IT Services e-Science and where relevant other bodies such as the former EuroDSD programme and the ESPE DSD group who may legitimately use it. It references external security documentation and standards, including IT Services e-Science corporate security policy and where relevant the security policies and procedures of other organisations such as the NHS.

# System Level Security Policy

1. **Name of system**: [I-DSD]
2. **Responsible Owner:** [**John Watt**]
3. **System’s Caldicott Guardian or Data Controller**:[Richard Copland]
4. **Overview of IT Services e-Science Security Systems:**

Security of the system shall be governed by the corporate security policy of [IT Services e-Science, University of Glasgow]

The system’s responsible security manager is [Dr John Watt]. Dr Watt is responsible for:

* Defining local access control policies on specific local resources (assets)
* Implementing and enforcing local access control policies;
* Working with University of Glasgow IT Support personnel on networking and university-wide firewalls and filters;
* Implementing local sub-network firewalls and locking down IP address ranges;
* Patching and updates to local assets including both operating system updates; middleware updates and anti-virus software updates.
* Working with local developers on deployment and management of security-oriented solutions providing access to assets;
* Security sign-off/accreditation of systems giving access to assets;
* Continuous support for staff security and training;
* Continuous monitoring and evaluation of IT Services e-Science assets and their interfaces with the wider university and access by remote collaborators;
1. **System Structure**

**5.1 Overview**

The security systems in place at IT Services e-Science have been developed by [Dr. Watt and the IT Services e-Science staff] through numerous large scale projects in the area of collaborative research with specific emphasis on security. (More information on these projects is available at [www.nesc.ac.uk/hub/projects](http://www.nesc.ac.uk/hub/projects)). These systems will be adopted by the I-DSD Network with continued implementation support by IT Services e-Science Glasgow and [Dr Watt, Mr Jipu Jiang][[1]](#footnote-1).

* 1. **System Components**

The I-DSD System comprises:

1. Front end portal for access to client interfaces;
2. Mid-tier server hosting services that allow secure access to and upload of I-DSD core data sets with further services being developed for further collaborative tools, e.g. wikis and tools for bioinformatics analysis etc;
3. Back-end database hosting contributed I-DSD core data;
4. Back-end database for other information/data on I-DSD, e.g. wiki.
5. Local authorisation server hosting policies for access to and use of I-DSD data by recognised researchers;
6. Detailed information on portal on I-DSD data set formats and information sheets;
7. Server redundancy for fault tolerance and failover;
	1. **System Processes**

The I-DSD system supports the following processes:

1. Researchers can securely access a portal hosted at IT Services e-Science which allows to: upload I-DSD data sets; search over contributed data sets and delete/edit data sets (subject to privileges).
2. To support this each recognised researcher is registered with IT Services e-Science Identity Provider and assigned roles that allow data upload and/or query capabilities. The information on individuals in I-DSD and their privileges are maintained and agreed by a named panel that currently consists of Prof Ahmed and Dr Bryce.
3. The I-DSD core data sets themselves adhere to a recognised core data definition available at <http://www.gla.ac.uk/idsd>. We note that none of this data includes identifying information on the patients or cases being contributed.
4. All access to the I-DSD system is monitored, logged and audited.
5. I-DSD researchers are able to select their own username and password to access the I-DSD registry. The actual access itself is achieved through a web browser. The I-DSD system is set to automatically log people off if there are periods of inactivity greater than 5mins.
	1. **System Authorised Purpose**

The ultimate aim of I-DSD is to develop and maintain a register that facilitates clinical and basic research that will ultimately improve long-term outcome of patients with conditions that are associated with disorders of sex development. This registry will eventually evolve to become a complete Virtual Research Environment (VRE) for DSD research.

* 1. **System Authorised Users**

Currently there are over 100 registered researchers associated with the I-DSD project. The access to the I-DSD resources (data sets and services) is agreed upon by Prof Ahmed, and Dr Bryce and is in accordance with appropriate data sharing policies and consent levels across the I-DSD project. The privileges of these individuals are enforced by a local security policy at IT Services e-Science currently maintained by Dr Watt and Dr Jiang[[2]](#footnote-2). A simple spreadsheet is used for keeping track of the local role based access control security policy which the access policy ultimately enforces. This set of registered users is expected to scale as I-DSD becomes the pre-eminent resource for DSD research.

The I-DSD security policies themselves have been designed to be simple but offer sufficient fine grained security for the I-DSD researchers to undertake their research. Each I-DSD collaborator is assigned one or two roles which allow secure access to upload data to the registry or to search for and access data in the registry, or both. It is not possible for researchers to do anything that their privileges (roles) do not allow, i.e. there is no arbitrary querying of the database. Instead standardised core data with standardised forms/query interfaces exist and access control is enforced accordingly.

* 1. **System Network**

The I-DSD system exists on a separate sub-network of the University of Glasgow. The I-DSD system resources are isolated from the wider campus network and can only be accessed through defined and enforced policy enforcement points. The core servers will only accept connections from recognised and trusted IP addresses.

* 1. **System Security**

The I-DSD system and its hosting at IT Services e-Science in Glasgow have the following security measures in place. Firstly, the actual servers used in I-DSD are physical protected. These servers exist in a specifically established windowless server room set up at IT Services e-Science in Glasgow. This has swipe card/PIN access for recognised individuals only and is kept locked at all times. The Kelvin Building itself has CCTV and janitor protected access/entry to the building more generally.

The I-DSD system servers themselves have all unnecessary services turned off, e.g. Telnet, FTP. The firewalls and IP chain rules are set such that they do not allow incoming connections from any networked resource other than the locally defined and enforced access control point, i.e. where the access and usage policy is enforced. All of these servers have strong password policies that are defined and enforced.

All data is strongly encrypted when uploaded from remote client systems or returned to remote client systems using X509 based public key infrastructure keys. The IT Services e-Science at Glasgow does not in itself have any paper based documentation on the I-DSD data or cases registered other than the digital and non-identifying core data set itself.

All of the I-DSD servers (which are all Linux based) are patched regularly. Indeed all resources at IT Services e-Science are patched as soon as potential threats or security holes have been identified. We proactively monitor such information and undertake our own in-house testing, e.g. for SQL injection attacks amongst others. The patching we undertake includes patching of the underlying operating system (typically Fedora core); the middleware and services that are deployed and comprise the I-DSD system as well as anti-virus software that is used (Sophos).

IT Services e-Science continue to achieve and strive for compliance with security management practices as set out in BS7799/ISO 17799. We are internationally recognised for the leading research we undertake in fine grained computer security.

* 1. **Risk assessment and audit arrangements**

The I-DSD system is continually assessed for risks and potential threats. The risk assessment we undertake is based upon standard risk assessment models. This includes:

* identifying all information and resources that needs to be protected;
* identifying all sources of risk;
* determining the probability of occurrence of each risk item on each protected item;
* quantitatively and qualitatively assessing the likely impact on business of the occurrence of each risk item on each protected item;
* identifying actions that can mitigate the effects of each risk item;
* quantifying the cost of implementing mitigating actions.

These risks include addressing changes in personnel and identifying and cataloguing any deficiencies, including security or confidentiality matters of the I-DSD system. This *process* of security is fed into both wider information security mechanisms and across many projects at IT Services e-Science

In the case of I-DSD, we are fully aware that the risks associated with compromises to the I-DSD system represent major concerns and will have a serious and negative impact upon IT Services e-Science and our collaborators both in the UK through organisations such as the NHS and internationally. We therefore proactively seek to identify and protect ourselves against all potential threats, both real and perceived. We believe that the security systems we have designed and deployed that compromise the I-DSD system represent the current state of the art in inter-organisational collaborative systems.

We are involved in several other projects with the NHS with key staff awarded NHS Honorary Contracts after undergoing Disclosure Scotland background checks. We also liaise extensively with the NHS and their IT and security support staff, on the solutions that we have produced that provide secure data access.

All access to the system is logged and regularly audited. This includes authorised access and usage by the I-DSD researchers. We also continually monitor attempts from inside and outside the university to access our systems.

1. **System Recovery Mechanisms**

The system has the following resilience arrangements in place:

1. I-DSD research data is backed up daily to a separate local database at IT Services e-Science;
2. Separate local copies of data are backed up to DVD and stored remotely in a secure and locked office at Yorkhill hospital;
3. The portal server and associated severs hosting services which provide access to the I-DSD data have built in redundancy, i.e. should any one of them fail, then local back-up servers exist and will automatically deploy.
4. The IT Services e-Science server room has UPS support and will gracefully shut down in case of power outages.

In the event of an electronic system failure the database system and associated servers comprising the I-DSD system can be restored. For major incidents, e.g. fires, the data and systems can be re-established using data kept offsite.

1. **Data Destruction**

Data existing within the I-DSD registry can be edited or deleted by the owner of this data. This may be the person who uploaded the data but can also be a local researcher working on behalf of an I-DSD investigator for example. A patient can instigate this deletion if they so wish. Data deletion results in removal of the data from the back end database and any local replicas of this database. We emphasise that this data has been specifically defined to not include any identifying information on patients.

1. **Responsibility for I-DSD SLSP**

This SLSP is the responsibility of Dr. Watt and shall be reviewed on an annual basis as part of the risk assessment and audit processes in place.

This SLSP has been made available to the Lead organisation Caldicott Guardian Dr Richard Copland, the System IT security Manager Dr John Watt and the I-DSD Group.

1. Those involved in the implementation of the study may change for a variety of reasons e.g. staff turnover, new researchers etc. [↑](#footnote-ref-1)
2. Authorised users may change for a variety of reasons e.g. staff turnover, new researchers etc. [↑](#footnote-ref-2)