**System Level Security Policy (SLSP)**

**For the <<Project Name>> database**

**Version 1 – 22-Nov-2018**

### Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Version Author(s) and project roles | Reason |
| 1 | 22-Nov-2018 | Allan Walker  CDMA Developer | * Initial creation |

Introduction

This System Level Security policy will help to demonstrate an understanding of information governance risks and commitment to address the security and confidentiality needs of the <<Project Name>> study.

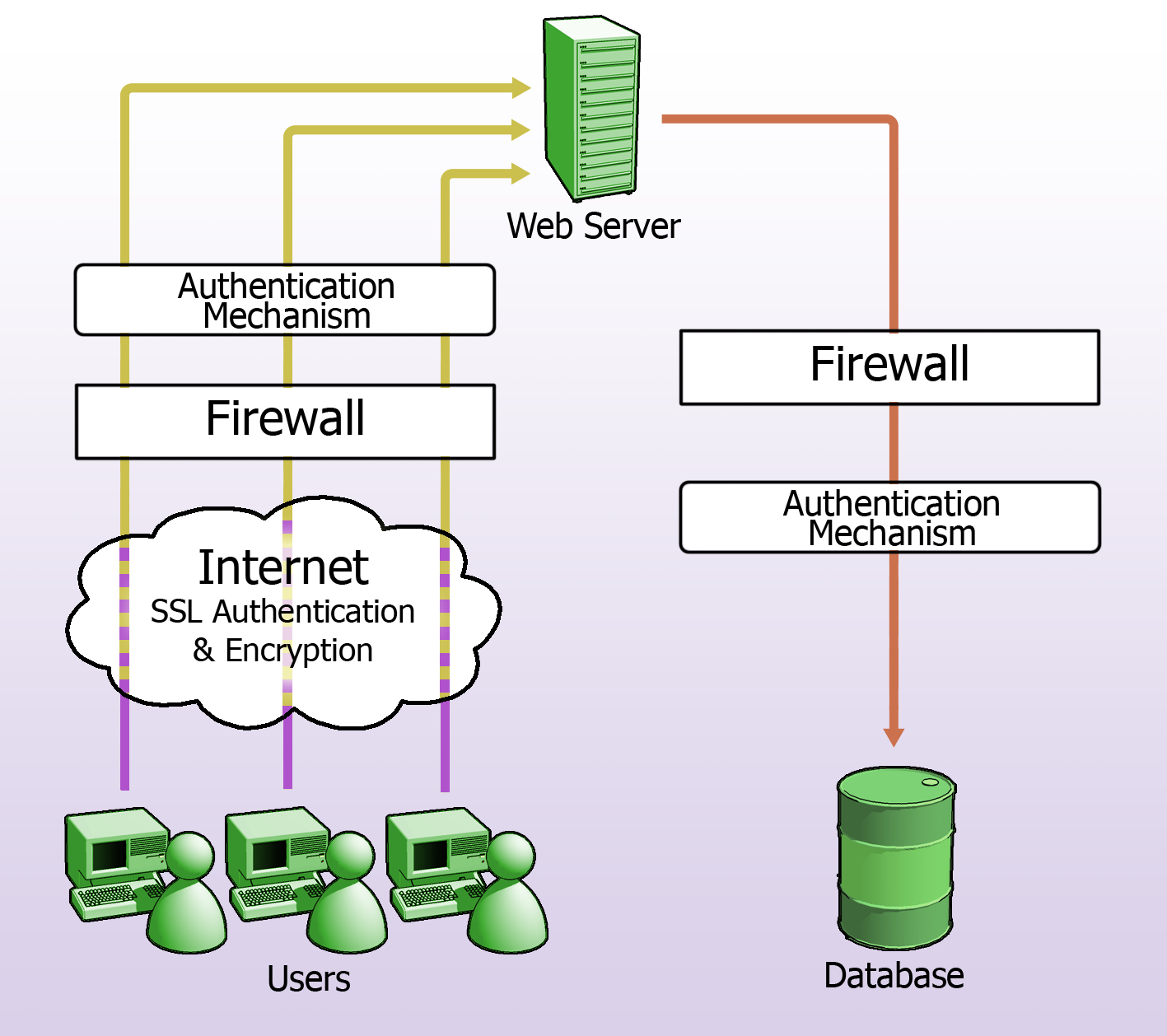
It will contain a considered and specific view of the range of security policy and management issues relevant to the <<Project Name>> Study.

**System Details**

1. The system shall be known as the <<Project Name>> Study database.
2. The system’s responsible owner shall be Chief Investigator of the <<Project Name>> Study.
3. The system’s Caldicott Guardian shall be NHS Lothian’s Caldicott Guardian.

**System Security**

1. Security of the system shall be governed by the ECTU SOPs.
2. The system’s responsible security manager shall be the head of the Data Management Systems team within Edinburgh Clinical Trials Unit.
3. The security manager duties shall include:
   1. Paper-based sections of the system
      1. Ensuring confidential and personal data is stored securely in a lockable cabinet.
      2. Ensuring procedures are in place to provide appropriate training for accessing and storing personal and confidential data.
   2. Electronic sections of the system
      1. Ensure new users are added appropriately to the system.
      2. Ensure procedures are in place to provide appropriate training for users.
      3. Ensure that access to the system is limited only to those users who have a current, identified need to access the system.
4. The system shall incorporate the following security measures
   1. Physical security measures.
      1. Access to the ECTU Offices is via an electronic keypad. Confidential paperwork is located in a staffed office. The cabinet within this office is also locked when not in use.
      2. The database is stored on a SQL Server. This is held in a locked server room with access restricted to essential personnel only.
      3. The Web server serving the web-application front end is similarly located on a University maintained server. As before, such servers are held in locked server rooms with access restricted to essential personnel only.
      4. The Image store is similarly located on a University maintained server. As before, such servers are held in locked server rooms with access restricted to essential personnel only.
   2. Logical measures for access control and privilege management
      1. Access to the SQL Server database is via the application only, with the exception of the study statistician who is granted read-only access to the database. Authentication for the statistician is provided via the University of Edinburgh’s server and authorization to access the database is stored within the SQL Server itself. Usernames and 8 character alphanumeric passwords are issued to users by the ECTU team. Users are asked to change their password when they first log in.
      2. Access to the web application which provides the interface for data entry is controlled by role-based password protected authentication. Passwords must be at least 8 characters long. Passwords are stored in the database and are encrypted
      3. Access to the image store is controlled by Windows authentication. Images can only be sent to the Image store via the application. Read-only access is granted to a small number of users who are authenticated via Windows Authentication using their registered Edinburgh University user credentials.
      4. All data transmission over the internet is secured by way of a Secure Sockets authentication and encryption Layer. This layer uses a 2048 bit RSA encrypted key.
   3. Audit
      1. Paper-based system
         1. Control of paper based data is outside the scope of this document
      2. Electronic system
         1. The <<Project Name>> Study database provides an audit trail for data modifications following ECTU SOPs.



**System Management**

1. The system shall be developed, maintained and implemented by the Data Management team within Edinburgh Clinical Trials unit.
2. The System shall be used by the <<Project Name>> study management team and by members of the <<Project Name>> Study research team. The trial management team is based at the Edinburgh Clinical Trials Unit. <<Project Name>> study Research team members are located at participating sites.

**System Design**

1. Description
   1. Members of the <<Project Name>> Study research team enter data directly into the trial database via a web-based front-end application. Research team members at each site are responsible for entering the data for that site into the system. The Edinburgh PI is responsible for entering details obtained from analysing scan data. SAE details, if recorded, are faxed to the ACCORD office.
2. Unauthorised access prevention
   1. Web browser access to data
      1. Remote access to data is provided via a user’s web browser. This ensures that data does not need to leave the physical estate, and is never stored on the user’s pc. All users need to authenticate before being able to access the data. Data is encrypted as it travels over the internet.
      2. The application partitions data according to the role of the researcher. Site researchers only have access to data entered for trial subjects associated with that site.
   2. Security Monitoring
      1. All IT services and the equipment they are hosted upon are remotely scanned on a regular basis to assess their security.

**Operational Processes**

1. A unique, unambiguous Subject No is assigned to each subject at the point they were entered into the trial.
2. If any datasets are transported outside the system they are encrypted using an industry standard encryption mechanism.
3. The authorised users are those members of staff deemed by the ECTU management to be assigned to the <<Project Name>> study.

**System protection**

1. Back-up and Disaster Recovery Procedures for Computerised Systems
   1. Back up and Disaster Recovery is provided by the University of Edinburgh Virtual Server environment. This mechanism is tested periodically according to ECTU SOPs.
2. Data Sources
   1. Snapshots of the data are taken at fixed times for analysis purposes.

**System Level Security Policy Ownership**

This SLSP shall be the responsibility of the ECTU Data Management Systems team. It shall be reviewed whenever the <<Project Name>> study system or any of its components or processes materially change. Additionally, it shall be reviewed whenever the SOPs it is underpinned by change, or additional SOPs are introduced that affect this policy.

**Data Protection Registration**

The University of Edinburgh’s data protection registration no. is: Z6426984.