Document name:	*[ ]:Information security assurance – role based access*
Date created:	*13 March 2017*
Author:	*Jane Smellie*
Approved by:	

Requirement 321: Access controls and password management procedures

Technical access controls are built into the OptoManager IT platform. To ensure data is safeguarded, this functionality must be complemented by operational and managerial controls put in place in the Company. This document outlines the procedures for managing access to systems.

1. Scope of the procedure

This procedure provides guidance on how access to the OptoManager IT system is controlled.

2. Authorising Access to the System

The Clinical Governance and Performance Lead is responsible for ensuring that directors and subcontractors and their staff have appropriate access rights to the system where required.

3. Managing Changes to Access Rights

A. Joiners

As part of normal induction processes new staff required to use the computer system will be issued with a user name, password and access rights appropriate to their role.

B. Profile Changes

Whenever there is a temporary or permanent significant change in the way a person works, a review of their access rights must be carried out.

C. Leavers

When staff members leave permanently, their profile should be removed.

D. Locums

Locum staff should be given temporary log on details, the password for this log on should be changed once the locum has finished their contract of employment.

E. Forgotten Passwords

Any staff member who has forgotten their password should contact IG Lead.

F. Misuse

If any staff member suspects misuse for example if their password has been accidentally disclosed, this must be reported to the Clinical Governance and Performance Lead. Depending on the severity of the allegation an investigation maybe required and appropriate disciplinary measures taken.

4. Procedures for staff in relation to logging in to the system

Password must be changed after first login	[ ]
Password must contain at least 8 characters	[ ]
Password must contain a mix of alpha numeric characters	[ ]
Password must contain a mix of upper and lower case characters	[ ]
Passwords must be changed every 90 days	[ ]
Passwords cannot be reused	[ ]
Password can be changed at user request	[ ]

5. Local Audit

The management of access rights will be subject to internal audit to ensure that this procedure is being followed. The audit will be undertaken every 12 months and will be co-ordinated by the Clinical Governance and Performance Lead.

6. Requirements for periodic review of the procedure

The procedure will be reviewed annually taking into consideration changes in national guidance and changes made to the technical access controls in the OptoManager system.