Rotamaster System Level Security Policy

Version	**1.3**
Location	Policy Folder – Information Technology
Approving Committee:	Urgent Care 24 Executive
Date Ratified:	2010
Reference Number:	UC24POL27
Name/Department of originator/individual:	Joseph Okwu, IM&T Manager
Name/Title of responsible committee/individual:	Director of Service Delivery and Operational Performance
Date issued:	2010
Review date:	March 2016
Target audience:	Rotamaster Users

Version	Date	Control Reason
1.0	January 2012	Reviewed due to changes in the process of the system level security policy.
1.1	November 2012	Reviewed in line with annual information governance submission. Changes made to job titles.
1.2	March 2015	Reviewed in line with annual information governance submission.
1.3	June 2018	Reviewed in line with annual information policy review date. Medical director name updated.

Table of Contents

1. INTRODUCTION

Urgent Care 24 has adopted this System Level Security (SLSP) Template as a way of documenting the system management arrangements for Rotamaster. It covers the security and management procedures that are planned and in place for data collection, data handling, data storage, data analysis and data destruction of personal and sensitive information. Also detailed are the lines of accountability within Rotamaster. This policy has been developed in line with the Information Security Policy.

2. PURPOSE OF SLSP

The purpose of this Rotamaster System Level Security Policy (SLSP) is to provide those responsible stakeholders with an understanding of the information governance, risk and the commitment required to address the security and confidentiality needs of the Rotamaster system.

3. SYSTEM AUTHORISED PURPOSE

The purpose of the system is to store, transfer and apply employee information into an electronic online rota system.

4. SYSTEM DETAILS

- **Name of System:** Rotamaster
- **System Caldicott Guardian:** Sandra Oelbaum **(**Medical Director)
- **Information Asset Owner** (IAO)**:** Joseph Okwu (IM&T Manager)
- **Information Asset Administrator(s)** (IAA)**:** Majo Oommen (IM&T Support Officer)
- **Senior Information Risk Officer:** James Carr, (Director of Service Delivery and Operational Performance)

5. SYSTEM SECURITY

5.1 Network and Physical security measures

The Rotamaster system servers are housed at a secure data centre managed by IQUS that protects the servers in the event of failure to server hardware, network failure, process failure and environmental failure. The data centre servers are protect by an onsite firewall protecting the servers and local area network from outside users trying to connect directly to the local desktop and network infrastructure

Access to the server rooms is only authorised personnel from IQUS.

5.2 Logical measures for access control and privilege management:

All computer systems require logon credentials in order to access them. Users are required to enter their username and password to gain access to the Urgent Care 24 domain. Access from sites maintaining their own domain have their own security policies enforced for access control.

The Urgent Care 24 domain security policy enforces logon limits to 3 failed login attempts, should the login fail after the third attempt then the account will become locked. The IM&T department are the only authorised staff who can unlock the accounts and a security log file is maintained. Logs are monitored on a daily basis by members of the IM&T department and a weekly report is emailed to the SIRO detailing all security events.

Access to the Rotamaster application is controlled by usernames, passwords which are only issued to UC24 personnel through authorised starters and leaver's forms. Authorisation is needed from the Director of Service Delivery and Operational Performance and line managers before any changes are made by the IM&T department.

The Rotamaster application is I.P restricted and cannot be accessed outside the NHS N3 Network.

5. SYSTEM MANAGEMENT

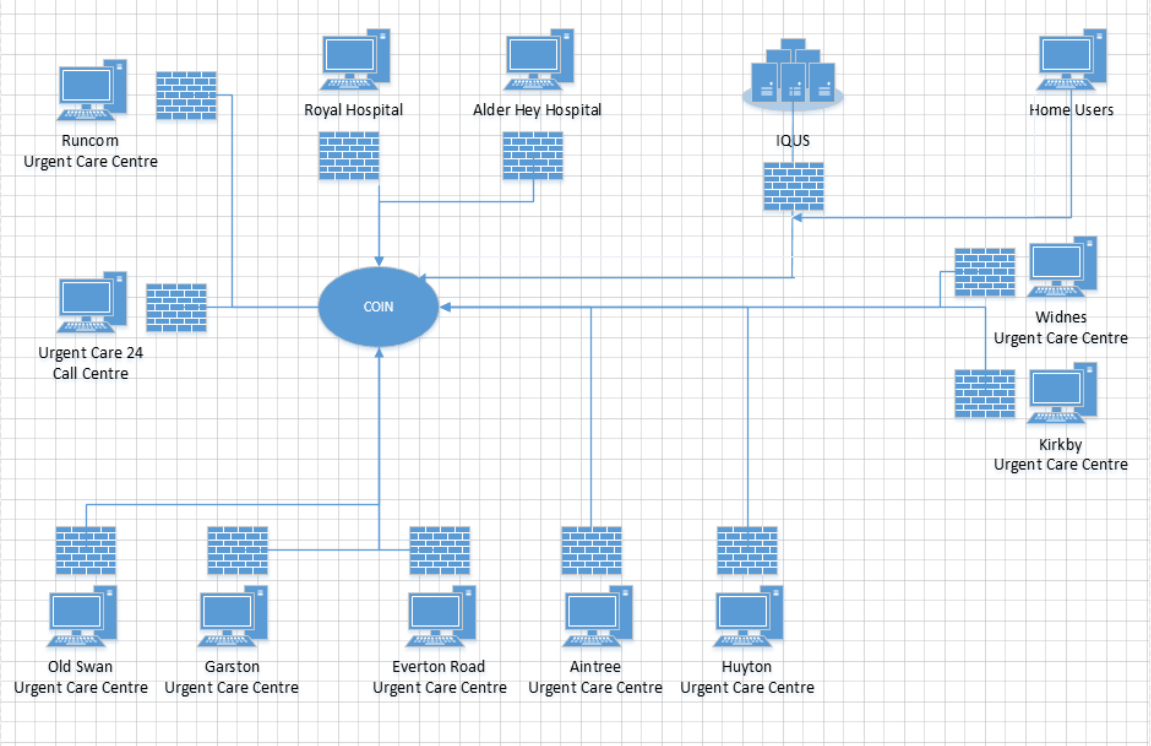
The system is housed and developed by IQUS Full address and contact details are shown below:

IQUS Limited
20A Appleton Court
Calder Park
Westfield
West Yorkshire
WF2 7AR
Tel: 0845 8340995

IQUS provide technical support across all of their hardware and software and lead on any new developments and changes required in the system.

6.0 SYSTEM DESIGN AND COMPONENTS

See the diagram below for overview of the system.



8.0 SYSTEM PROCESSES

8.1 Accessing the system

The Rotamaster system is accessed by entering the following link https://online.iqus.co.uk into the Internet Explorer address bar. Prior to users accessing the logon screen, users are prompted with site logon credentials which are only accessible to authorised members of the IM&T department. The back end Rotamaster database is only accessible to administration staff.

Users are then able to log into the Rotamaster application by entering their username and password. Usernames and passwords are only granted to users from the use of starter, leavers and change of rights forms. These forms authorised sign off from the SIRO and line manager before any access can be granted by members of the IM&T department.

Staff performing operational shifts will use the following link https://www.uc24.net to access the front end extranet of the Rotamaster application UC24.net. Accessing this site is restricted to only authorised UC24 personnel managed by the user of starters, leavers and change of rights user forms. Operational staff are able to manage their own rota and annual leave as well as apply and verify operational shifts.

8.2 Transfer and Process of Information

Information is processed through rota availabilities uploaded from the Rotamaster system to the UC24.net extranet. UC24 employees are then able to apply to the available shifts. Applications made by employees are received in the rota team NHS email account.

All requests are then manually inputted into the Rotamaster system. Shift verifications are then emailed automatically to the UC24 employees personal email account.

Daily and weekly rotas are then printed off and left with the supervisor to record all staff arrival and completion times of shifts. The rotas will contain no sensitive information.

8.3 Storage of Information

No information entered onto the Rotamaster system is saved on the local computers or servers, all information is saved directly onto the Rotamaster SQL database

9. RISK ASSESSMENT AND AUDIT ARRANGEMENTS

Any changes that have any impact upon the Rotamaster are required to go through the change control process. Within this process before implementation the change will be tested, risk assessed and approved by the Director of Service Delivery and Operational Performance.
All change requests will then be passed onto IQUS in order for the change to be made.

The system is risk assessed at regular intervals to ensure its integrity and performance for purpose. Any risk high risk identified will be added to the risk register for resolution by the IAA's.

An internal audit using the IMT audit checklist will be undertaken to ensure that procedures in this policy are being followed.

10. BUSINESS CONTINUITY

In the event of serious disruption or total system failure Urgent Care 24 will revert to a paper based system until the Rotamaster system will be back up and running. Staff will made aware of the extranet being down through the use of their personal emails. All applications for shifts will be done over the phone and recorded on a paper based rota system.

11. RECOVERY OF INFORMATION

In the event of information needing to be recovered weekly backups of employee details and rotas can be used to rebuild the Rotamaster system. Rota exports from the Adastra V3 system can be manually inputted back into Rotamaster.

The use of verifications and confirmations sent to the Rota team's mailbox can also be used for updates not recorded or lost to the daily rotas.

12. RETENTION AND DESTRUCTION

Information is retained and destructed in guidance with our records retention policy.

13. PASSWORD POLICY

New user accounts are created using a generic password. This is provided for the initial logon (This password will be provided during the induction process).The password will be prompted for the user to create a unique password.

Users are instructed **never** to share their password for any reason and if their password should become exposed they are to change the password immediately. If a user has forgotten their password they should inform the IM&T department or supervisor who will reset the password and initiate the same procedure for the induction process.

By default passwords for Rotamaster accounts have no alpha or numeric restrictions and have no date restrictions for change.