Telephony System Level Security Policy

Version	**1.3**
Location	Policy Folder – Information Technology
Approving Committee:	Urgent Care 24 Executive
Date Ratified:	2010
Reference Number:	UC24POL28
Name/Department of originator/individual:	Mark Brown, IM&T Manager
Name/Title of responsible committee/individual:	James Carr, Director of Service Delivery and Operational Performance
Date issued:	2010
Review date:	June 2018
Target audience:	IM&T, SIRO, Executives

Version	Date	Control Reason
1.0	30/12/2011	Reviewed in line with annual information governance submission.
1.1	05/12/12	Changes made to SLSP to reflect recent changes and developments to the telephony system.
1.2	03/04/2014	Reviewed in line of annual information governance submission.
1.3	June 2018	Reviewed in line with annual information policy review date. Medical director details updated.

CONTENTS

1. Introduction 3
2. Purpose of SLSP 3
3. System Authorised Purpose 3
4. System Details 3
5. System Security 3
5.1 Physical and network security measures 3
5.2 Logical measures for access control and privilege management 4
6. System Management 5
7. System Design and Components 6
8. System Processes 7
8.2 Transfer and Process of Information 7
8.3 Storage of Information 8
9. Risk Assessment and Audit Arrangements 8
10. Business Continuity 8
11. Recovery of Information 9
12. Retention and Destruction 9
13. Password Policies 9

1. INTRODUCTION

Urgent Care 24 has adopted this System Level Security Policy (SLSP) Template as a way of documenting the system management arrangements for business Telephony. 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 the telephone system. This policy has been developed in line with the Information Security Policy.

2. PURPOSE OF SLSP

The purpose of this 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 telephony within Urgent Care 24 (UC24).

3. SYSTEM AUTHORISED PURPOSE

The purpose of the telephony system is to support UC24 in its day to day operations of making and receiving calls from patients and healthcare professionals. The system records all calls made and received for training and monitoring purpose.

4. SYSTEM DETAILS

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

5. SYSTEM SECURITY

5.1 Physical and Network Security Measures

The telephony system is housed at the UC24 headquarters site in Wavertree Technology Park, Liverpool. Access to the building is restricted to UC24 personnel by inputting a four digit key code. The four digit code is changed in line with the internal policies of the Roy Castle Lung Foundation organisation.

The site is monitored 24/7 using CCTV located at the front and rear of the building, covering all entrances and exits, access to the CCTV recordings can only be authorised from the personnel at the Roy Castle Lung Foundation.

Access to the server room is restricted using a security key which is only allocated to members of the UC24 and Roy Castle Lung Foundation IM&T department. The UC24 server room doors are locked by a key which is only allocated to members of the UC24 IM&T department.

The servers are protected by an onsite firewall supported by Advanced Health and Care. The firewall protects the local area network preventing direct access from outside users to the desktop and server infrastructure. Malware and Anti-Virus security is installed on all servers and local machines to monitor any malicious viruses that could infect the local area network.

The Anti-Virus software is monitored on a daily basis and emails are sent to the IM&T department for any threats and vulnerabilities that have arisen.

5.2 Logical measures for access control and privilege management

All computer systems and servers require username and password logon credentials. The login credentials for the servers is restricted to only members of the IM&T department and relevant supporting companies, for this instance access to the telephony server is restricted to Solar and access to the call recording server is restricted to Xarios.

Although Xarios have access to the call recording server they require permission from the IM&T manager to gain access to call recordings. Access to call recordings is only granted to resolve any IM&T issues that have occurred. All supporting companies adhere to the information sharing agreements.

In order to access to the UC24 domain each user requires logon credentials. The domain security policy enforces logon limits to three 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.

User accounts can only be created by members of the IM&T department after receiving authorised new starter and change of user rights forms from the HR department. All authorisation needs to be approved by the UC24 SIRO and the appropriate line managers.

6. SYSTEM MANAGEMENT

The telephony system and call recorder is maintained by Solar Communications and Xarios. GAMMA provide the SIP telephone lines and a portal is available for the transferring of phone lines.

Full address and contact details are shown below:

Solar Communications
Unit L4,
Cody Court,
Salford Quays,
Greater Manchester,
M50 2GE
Tel: 0800 140 4080
Email: support@solar.co.uk

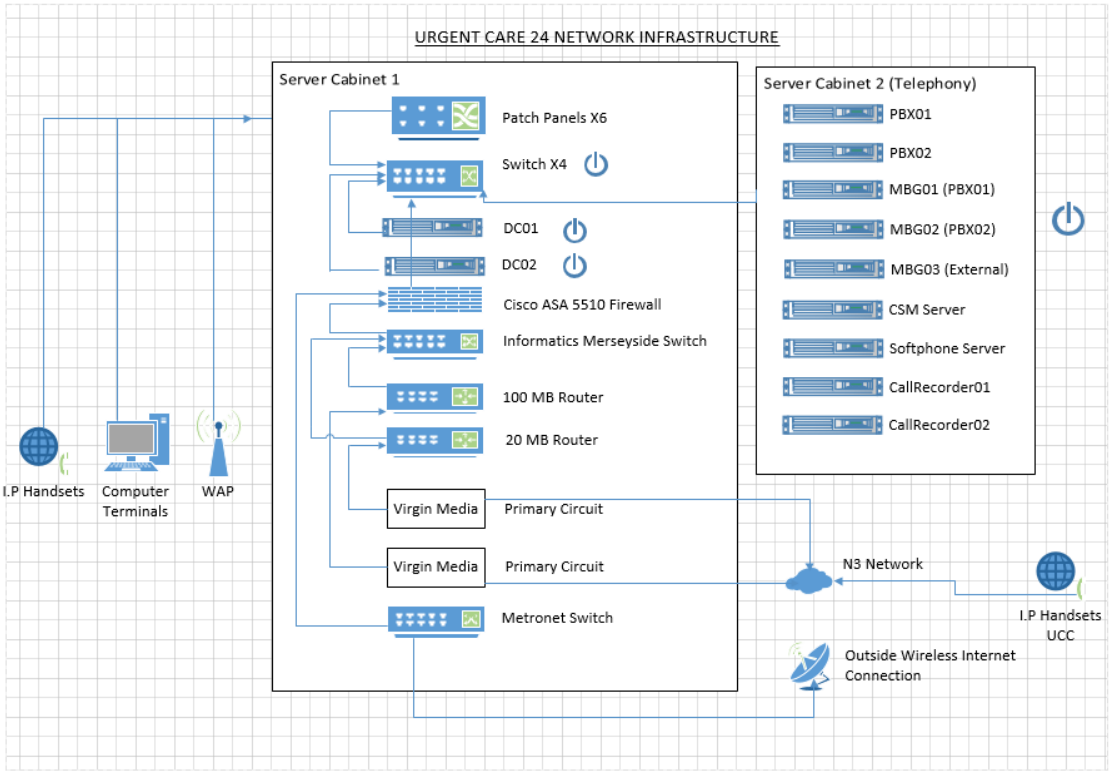
Xarios
Unit 7 Digital Park
Pacific Way
Salford Quays
Manchester
M50 1DR
Tel: 0845 373 6880
Email: support@xarios.com

GAMMA
For enquiries into the SIP telephone lines contact Solar Communications.

Solar and Xarios provide 24/7 technical support across all of their hardware and software. Solar and Xarios will continue to support and assist the UC24 IM&T department with any future developments.

7. SYSTEM DESIGN AND COMPONENTS

See the diagram below for the overview of the telephony system:



The telephony server equipment is housed onsite at the Urgent Care 24 headquarters premises in Wavertree. All I.P handsets have to be configured on the primary and secondary Mitel Controllers (PBX01/2)

The Mitel Border Gateways manage the I.P phone connections both internally within the local area network and also externally at the Urgent Care Centres.

In order to establish a connection all configured I.P Phones must be pointed to and enabled on the Mitel Border Gateways. Once a connection is made the I.P Phone will then establish a connection with the call recorder. All calls internal and external are recorded using extension side recording.

The I.P phones are routed using a primary 100mb Virgin Media connection onto the the N3 Network. In the event of failure to the 100mb connection a secondary 20mb connection is availble and will failover within 30 seconds. Both Virgin Media routers (100mb Primary and 20mb Secondary) are connected to separate UPS connections in the event of loss of power within the building.

The SIP phone lines supported by GAMMA and are routed over the NHS N3 Network and split over the 100mb Virgin Media connection and the 5mb Wireless Metronet Connection. Both connections are connected to separte telephony controllers allowing calls to come in across both networks and controllers at the same time. The approach provides a active/active connection were calls are sent alternatively to the primary and secondary controller.

Further resilience has been added by GAMMA by having traffic routed from both the Manchester and London headquarters. This setup is call load baring and offers further resillence by having two points of connection for the SIP lines with two separate network internet providers.

8. SYSTEM PROCESSES

8.1 Accessing the System

In order to access the telephony system all users are first required to logon to the UC24 domain. After logging onto the domain authorised users are able to access the call recordings, statistics and configure the telephony system. The access is restricted using usernames and passwords.

Configuration of the Mitel telephony system is restricted to members of the IM&T department. Members of the IM&T department will access the primary controller and secondary controller on the I.P address 192.168.220.1/2 using Internet Explorer. A username and password is then required before access is established.

Authorised users can access call recordings from two call recorders (call recorder1 is used for calls up to September 2013 and call recorder2 will show calls from past September 2013.

The call recorders are accessed from the web browser by typing callrecorder or call recorder2. The user will then be displayed with a username and password logon screen.

To run the statistics for compiling data to support the NQR reports users are required to logon into the CCM server (Contact Centre Management Server). This is accessed by typing the following link http://192.168.220.5/CCMWeb/ into the web browser.

Users are then prompted for a username and password and are able to export data directly to the local drive of the PC. All data is anonymised and only users to record telephony statistics.

8.2 Transfer and Process of Information

Information is processed when a patient, healthcare professional or mobile worker makes or receives call to and from UC24 and associated sites. The call and statistics are recorded for auditing and training purposes using the Mitel CCM and Xarios software held on the telephony servers.

Mobile workers have to use the dial through connection 0151 294 3215 to the telephony server in order to have a call recorded. All patient calls are required to be recorded. Configuration of a mobile phone for external call recording can only be made by the IM&T department.

Any voice recording needing to be transferred off the UC24 network are required to be stored on USB storage device with approved NHS encryption software.

8.3 Storage of Information

All information recorded is stored on secure servers connected to the UC24 domain. Call recording required to be archived are transferred onto a NAS drive connected to the UC24 domain. Voice recordings by made the mobile users are downloaded from the Voice Flex server and storage on the domain servers which are backed up on a 4 weekly schedule.

9. RISK ASSESSMENT AND AUDIT ARRANGEMENTS

Any changes to the UC24 telephony system 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 SIRO.

10. BUSINESS CONTINUITY

In the event of complete failure to the telephony system or evacuation of the building all calls to the patient and administration phone lines can be transferred to contingency mobile phones or external land lines. A call will need to be made to the Solar Communications support desk 0845 345 0700 were the call will be passed to available engineer in order to setup the landline phone transfer.

The phone system operates using a primary and secondary Mitel 3300 controller with separate network connections. The setup uses load barring which splits the calls over the two controllers and operates using two separate network connections. The primary controller is connected to a 100mb Virgin media Connection which is routed over the NHS network. The secondary controller is connected using a 5mb Metronet Wireless Connection which is routed outside the NHS network.

In the event of failure or loss of network connection to the primary controller all calls made to and from UC24 will continue to come into the secondary controller. All call handler agents will failover instantly to the secondary controller. (ACD Hot Desking is in place to automate this process.) The ACD agents will then fail back over to the primary controller once restored. The primary and secondary controller are connected to separate UPS in the event of loss of power to the building. The network routers Virgin Media (100mb Primary) and Metronet (5mb) secondary are also connected to separate UPS and will maintain operations in the event of loss of power until the main power to the building has been restored.

In the event of failure to either the controllers or network connections an alert will be sent Solar Communications and the supporting network connections provider (Primary Connection – Informatics Merseyside, Secondary Connection – Solar Communications).

If any failings are noticed from patients or operational staff the first point of call is to contact the Solar Communications Service desk 0845 345 0700 to help identify the problem. If the primary connection has failed a call will need to be made to the Informatics Merseyside service desk on 0151 296 7777.

The phone system contingency has been designed to reduce the time required of out of hour's staff interaction and to continue operations in the event of network failure.

At present there is no secondary backup call recording server if the primary server were to fail. All calls will fail to be recorded until the issue is resolved or the call recording server has been repaired or replaced.

11. RECOVERY OF INFORMATION

To help prevent loss of data the call recorder has been setup to a network NAS drive enabling storage over multiple hard drive disks.

12. RETENTION AND DESTRUCTION

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

13. PASSWORD POLICIES

Users are instructed never to share their password for any reason and if there password should become exposed they are to contact the IM&T department immediately to change the generic access password to these systems.