Property of Urgent Care 24 Uncontrolled copy when printed
Not to be used without permission of the Board of Urgent Care 24

Network System Level Security Policy

Version	**1.5**
Location	Policy Folder – Information Management & Technology
Approving Committee:	Urgent Care 24 Executive
Date Ratified:	2010
Reference Number:	UC24POL25
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
Next Review date:	July 2019
Target audience:	All Employees

Version	**Date**	**Control Reason**
1.1	29/12/2011	Reviewed in line with annual information governance submission.
1.2	01/12/2012	Reviewed in line with annual information governance submission. Changes made to employee job titles.
1.3	28/07/2014	Reviewed in line with annual information governance submission
1.4	28.02.2015	Reviewed in line with annual information governance submission

1.5	04/06/2018	Reviewed in line to Annual Review Date. Changed names of System Caldicott Guardian; Information asset owners and information Administrators.

CONTENTS

1. INTRODUCTION

Urgent Care 24 (UC24) has adopted this System Level Security (SLSP) Template as a way of documenting the system management arrangements for the UC24 network. 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 UC24 network. 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 asset owners and administrators with an understanding of the information governance, risk and the commitment required to address the security and confidentiality needs of the UC24 network.

3. SYSTEM AUTHORISED PURPOSE:

The purpose of the UC24 network is to provide authentication to users to securely access, store, maintain and transfer information in accordance to information governance guidelines and procedures. The UC24 local area network (LAN) allows access to services including email, telephony, internet, intranet, clinical applications and wider area networks (WAN). The network is essential to UC24 for carrying out its day to day operations.

4. SYSTEM DETAILS

- **Name of System:** Urgent Care 24 Local Area Network
- **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 UC24 LAN infrastructure 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 (RCLF).

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 RCLF.

Access to the server room is restricted using a security key which is only allocated to members of the UC24 and RCLF 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 server infrastructure is protected by an onsite firewall supported by Advanced Health and Care (AHC). The firewall protects the LAN preventing direct access from outside users to the desktop and server infrastructure. Malware and Anti-Virus software is installed on all servers and local machines to monitor any malicious viruses that could infect the LAN.

The Anti-Virus software is monitored on a daily basis and emails are sent to the IM&T department of any threats and vulnerabilities that have arisen. Weekly scheduled scans are undertaken on the domain servers and the workstations connected to the UC24 domain.

5.2 Logical measures for access control and privilege management

All computer systems require logon credentials in order to access the UC24 domain. 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 and a security log file is maintained. Logs are monitored on a daily basis by members of the IM&T department and reports of any breaches in security are emailed to the SIRO.

All users allowed access to the UC24 domain have varying levels of access based upon the user permissions they have been assigned. All permissions are assigned and changed through the use of the starters, leavers and change of rights user forms. Authorisation from the SIRO and line managers is required before any user accounts are created, deleted or altered.

Third party and supporting companies requiring access to the servers have to contact the UC24 IM&T department. All access is logged and recorded. Temporary user accounts will be created and disabled once the access is no longer needed.

6. SYSTEM MANAGEMENT

The LAN infrastructure (Switches, Domain Servers, Server UPS, and Firewall) is maintained by AHC, UC24 and Informatics Merseyside (IM). Full address and contact details of their main office are shown below.

Advanced Health and Care
Unit 4 Eurogate Business Park
Ashford
Kent
TN24 8SB
Tel: 01233 722667

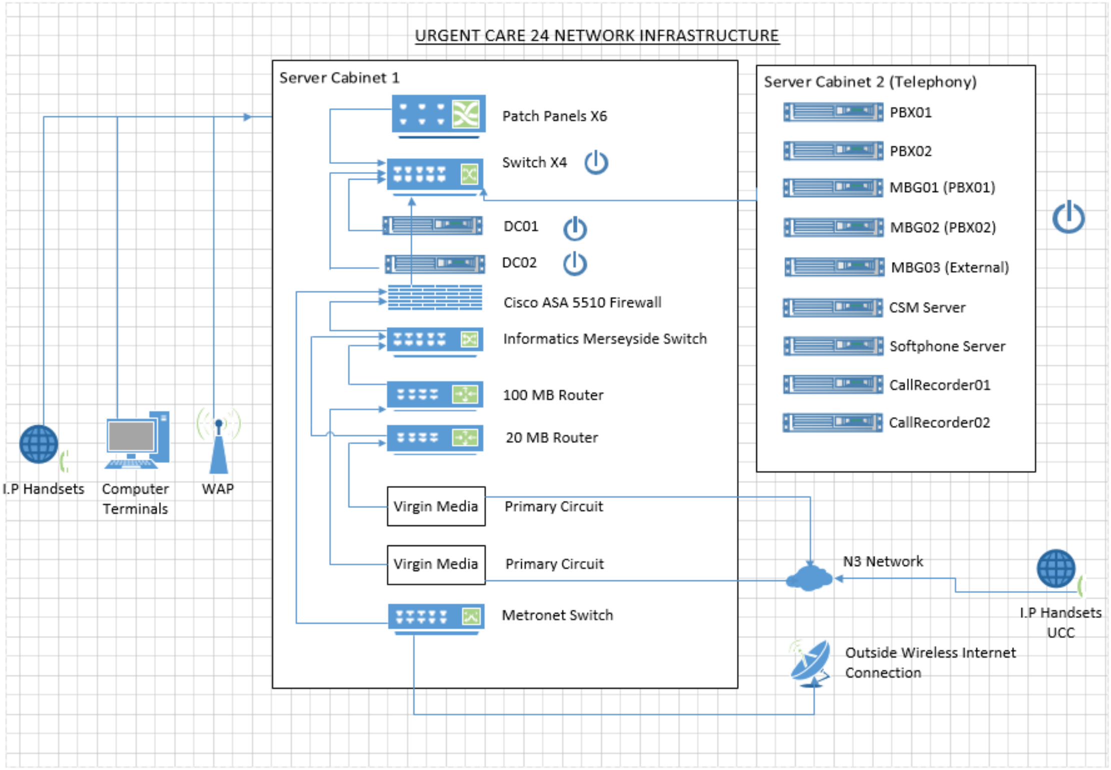
Informatics Merseyside
Stephenson Way
Wavertree Technology Park
Liverpool
L13 1HD
Tel: 0151 296 7777

AHC provide 24/7 technical support across all of their hardware and software. IM support the routers that allow connection from the LAN to the WAN (N3/COIN network).

Both parties 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 Urgent Care 24 local area network



The LAN is housed onsite at the UC24 headquarters premises in Wavertree and consists of a primary and secondary domain controller (DC01 192.168.110.10/DC02 192.168.110.11) that supports key server functions including Active Directory (authentication, creation and management of user accounts), File Directories & Security (file access, user home drives and shared organisation drives), DHCP (allocation of dynamic I.P addresses to hosts connected to the network), Backup Exec (four weekly schedule of data backups), Anti-Virus and Print Servers (networked organisation printers)

The LAN server infrastructure is connected to an Uninterrupted Power Supply (UPS) in the event of loss of power to the building. The LAN connects to the WAN (N3 / COIN NHS Network) using a primary 100mb Virgin Media connection. In the event of failure to the primary connection a secondary 20mb connection is availble and will failover within 30 seconds. The UC24 firewall is routed to the virtual I.P address 10.213.237.238 which can transfer between the primary and secondary router in the event of failure. 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.

UC24 also has a wireless access point which is used to connect staff mobile devices to receive emails and provide external users with internet access if required. Access is restricted using a password which is only available to the IM&T department. Approval is required by the SIRO before any employee or external user is granted access. The WAP does not allow access to the Urgent Care 24 domain or file infrastructure.

For full details on the telephony infrastructure and wireless Metronet routers refer to the Urgent Care 24 Telephony SLSP.

8. SYSTEM PROCESSES

8.1 Accessing the System

The LAN is accessed using computer terminals connected to the UC24 domain at the Wavertree headquarters. All terminals require a username and password which is allocated to new staff members using new starter forms.

Each user will have a varied level of access depending upon their job role with the organisation. After logging onto the UC24 domain users will have access to the Internet, Intranet, shared file directory (This will vary depending on the user), Microsoft Office, Adastra V3.24 Smart-Client, Emis Web, Rotamaster and Mitel Contact Centre Client. Please see SLSP documents for Adastra, Emis, Rotamaster and Telephony)

8.2 Transfer and Process of Information

Information that is stored and accessed within the UC24 domain is held within restricted folders on the organisation shared file directory. When a user account is created an individual home drive is assigned allowing the user to store personal and sensitive information. All access to the personal drive is restricted to only that particular user and IM&T administrators.

Information that is shared on the network is held within departmental folders. Each department has their own separate folder. Only users within the department will have access to the information. The information is current and in use. Archive folders are available for all users and departments if the information held is no longer relevant.
Information needing to be transferred outside the network will be stored on encrypted USB storage devices. All USB storage devices are encrypted to 256 BIT AES standard in guidance with the encryption policy.

All use of external USB storage devices are prohibited on the UC24 network unless authorisation is approved by the IM&T department. Please refer to Encryption SLSP for further information regarding the use of USB storage devices.

8.3 Storage of Information

All information stored on the LAN is backed daily on a four week cycle. The information is backed up to encrypted DAT tapes. For information relating to the storage of call recordings please refer to the Urgent Care 24 Telephony SLSP.

9. RISK ASSESSMENT AND AUDIT ARRANGEMENTS

Any changes that have any impact upon the LAN are required to go through internal/external 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.

Audit arrangements using the virus and malware software are setup to automatically manage and prevent malicious codes, viruses, Trojans and external hackings. Automatic scans and updates are set to be carried out on a weekly basis. Operating systems patches and updates are managed by a group policy script. Any additional updates will be carried out by members of the IM&T department.

The network is checked daily by members of the IM&T department for viruses, malware, vulnerabilities, data back ups and server logs. Email alerts are sent to members of the IM&T department of any threats or vulnerabilities that have been found.

10. BUSINESS CONTINUITY

The LAN has two domain controllers, a primary and secondary controller. The secondary controller acts as a redundancy to the primary controller in the event of failure and will take over the roles and responsibilities to keep the LAN operating with minimal disruption. Each controller is connected to a separate UPS in the event of loss of power to the building.

Each controller has its own Active Directory service which mirrors the other server, this enables user accounts and permissions to stay protected in the event of server failure. The LAN is maintained until such a point that the failed server is repaired or replaced.

Each server has a mirrored Raid 5 setup to provide resilience should one or more of the hard drives in the array suffer a failure during operation. This level of resilience will provide protection to loss of data and performance of key server functions.

If both servers fail due to equipment failure all staff will revert to using paper based system. A call will need to be made to the AHC service desk 01233 722 667 to resolve the issue. Users will report no access the UC24 domain, shared file directory, software applications and Internet.

If the Internet is just affected and users can still access the shared drives contact the IM&T service desk 0151 296 7777 and report that the Primary and secondary Virgin Media routers that provide access to WAN (N3 Network) have lost connection. Upon loss of connection to the Virgin Media routers the network team at Informatics Merseyside will be automatically notified. UC24 will continue without network access until the issue is resolved. Access to the Adastra application will remain operational as long as the N3 network is available.

11. RECOVERY OF INFORMATION

All information stored on the network is backed up daily by members of the IM&T department. The data is stored on encrypted DAT tape technology with a four week retention period. All data recorded is stored within a safe at the Wavertree Headquarters.

12. RETENTION AND DESTRUCTION

Content is subject in accordance with UC24 Records and Retention Policy.

13. PASSWORD POLICIES

When new user accounts are created a generic password 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 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 who will reset the password and initiate the same procedure for the induction process.

All users have three failed login attempts before the account is locked. Only members of the IM&T department are able to unlock user accounts.

By default, passwords for internal accounts are set to expire after 30 days and have a minimum 6 letters.