NHS
Urgent Care 24

Property of Urgent Care 24 Uncontrolled copy when printed

Not to be used without the permission of the Board of Urgent Care 24

CHANGE CONTROL AND MANAGEMENT POLICY

Version	V1.1
Location	Policy Folder – Information Technology
Approving Committee:	Executive
Date Ratified:	March 2012
Reference Number:	UC24POL62
Name/Department of originator/individual:	Kate Hindle Head of Operations & Performance, Reviewed by Stephen Mather Service Manager
Name/Title of responsible committee/individual:	Service Managers
Date issued:	February 2012
Review date:	February 2015
Target audience:	All employees

Version	**Date**	**Control Reason**
1.1	23rd November 2012	Reformatted old Policy to new format. Altered Job Titles for IT Lead, Director of IM&T to Director of Service Delivery and Operational Delivery and IM and T Lead. Added responsibilities to Service Manager with responsibility for Information Governance section 4.0.
1.2	24th February 2015	Reviewed in line with annual information governance submission. Job title changed for Kate Hindle to Head of Operations & Performance & IM&T Lead to IM&T Manager

Contents

Appendices

1.0 PURPOSE

1.1 Information and information assets are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available to those who require them and accurate to support service delivery and business continuity.

1.2 Urgent Care 24 acknowledges that it must demonstrate to third parties its' expertise in security technology and implementing it. To achieve this, it is recognised that Urgent Care 24 must protect its' own and associated assets.

1.3 The main aim of this Change Control and Management Policy is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the organisation. It also aims to ensure that all relevant employees, departments or external organisations are aware of any proposed and actual changes. The procedure outlines the standards to be used for the testing of software and hardware by the organisation.

1.4 This policy should be read in conjunction with the following policies: Urgent Care 24 Information Governance Corporate Policy and Strategy (UC24POL8), Urgent Care 24 Risk Management Policy (UC24POL2). These standards, procedures and policies will be used as part of the Information Security Management System (ISMS) within the organisation.

2.0 SCOPE

2.1 This policy applies to all employees of Urgent Care 24.

3.0 RESPONSIBILITIES

3.1 All employees have a responsibility to adhere to the terms and conditions of this policy.

3.2 Line Managers and Heads of Departments who are specified as the responsible people within the policy must ensure the correct procedure is carried out.

3.3 Any queries on the application or interpretation of this policy must be discussed with the author/s prior to any action taking place.

3.4 This policy will be reviewed on an annual basis and updated as appropriate.

4.0 PARTICULAR RESPONSIBILITIES WITHIN THIS STANDARD ARE DEFINED AS FOLLOWS:

- **Review and maintenance**: Service Delivery Managers
- **Approval:** Information Governance Steering Group
- **Adoption:** Executive Directors, Line Managers and Heads of Department
- **Compliance:** All staff and contractors (in scope)
- **Monitoring:** Information Asset Owners, Service Delivery Manager with responsibility for Information Governance

5.0 INTERNAL CHANGE APPROVAL PROCEDURES

5.1 Overview

5.1.1 The operational change control process covers initiation of change, control of change, record keeping and decision making for all aspects of change to the organisations information systems.

5.1.2 The processes are intended to ensure minimum time impact on the actual changes themselves. The process should not slow down the start or pace of change. There are two processes;

a) For new projects and large changes, there is the **Major Change Process**
b) For smaller changes, there is the **Minor Change Process**.

5.1.3 Each process is described in the following sections.

5.2 Record Keeping and Auditing of Changes to Systems

5.2.1 An audit trail will be kept. Each change will have a form which will record progress at every stage; this is the responsibility of the Information Asset Owner supported by the Service Delivery Manager with responsibility for Information Governance. The form will be the basis of the final implementation change control decisions process.

5.3 Test System

5.3.1 Wherever possible, change and implementation work should be tested on the test system. This should be kept as close as possible to live system in configuration.

5.4 Who makes Change Control decisions?

5.4.1 The decision as to whether a change is deemed to be Major or Minor will be taken by the Line Manager or Head of Department and the relevant Executive Director.

5.4.2 The decision as to whether a Major Change will be implemented on to a live system will be ratified by the Executive Directors.

5.4.3 The decision to implement Minor Changes lies with the appropriate Line Manager or Head of Department and the IM and T Manager. The outcome of the decision making process will be communicated with all relevant Line Managers, employees and the appropriate Executive Director.

6.0 INTERNAL CHANGE IMPLEMENTATION PROCESS

6.1 Classification

6.1.1 There are two different levels of change which affect the organisation's computer based information systems. These are classified as follows:

a) Major changes to systems (the **Major Change Implementation Process**). This process covers changes which will have a major effect on the information systems, for example replacing an existing system such as telephony provider or Rotamaster or upgrading operating systems to newer versions.

b) Minor changes to existing systems (the **Minor Change Implementation Process**). This process covers minor changes to systems which are any change not covered by the Major Change Implementation Process.

6.1.2 The choice of process for each piece of work will be made by the Line Manager or Executive Director proposing the change.

6.2 The Major Change Implementation Process

6.2.1 This process involves:

- The steps in part A of the Major Change Record Form (MaCRF) will be completed by the requester and the system owner.

- Part B of the MaCRF will be filled in by the requester and owner and passed to the Director of Service Delivery and Operational Performance.
- The MaCRF will be presented to the Executive Directors for approval or further clarification.

- If approved, the IM and T Manager will arrange for the implementation of change.

- Prior to implementing the change the system(s) will be safeguarded by taking steps to ensure a fall-back position if necessary. All relevant technical, operating and user documentation will be updated by the owner as far as possible.

- Once implemented the change must be monitored by the requester, the owner and a member of the IT team to ensure that there are no problems. If a problem does occur then the fall-back procedure as documented in the MaCRF will be implemented. The IM and T Manager will be responsible for these arrangements, having informed all parties involved.

- If the change is not approved feedback will be provided to the requester/owner in order that they may take the appropriate action, such as any alteration in plans.

- Once implemented all relevant technical, operating and user documentation will be further reviewed and updated as appropriate. This is the responsibility of the owner.

- The complete MaCRF will be retained for no less than ten years for future reference.

6.3 The Minor Change Implementation Process

6.3.1 The designation of a piece of work as a Minor Change will be made by the IM and T Manager.

6.3.2 The Minor Change Record Form (MiCRF) should be completed by the requester who should give the following information:

a) The category (such as hardware, software, operating system)

b) A brief description of the change required
The employee who makes the change should also later note any intermediate changes that are needed to be made to make the change successful, i.e. patch or upgrade to web-browser.

c) The date by which the change is required (go-live).

6.3.3 Approval will be given by the relevant Line Manager and Executive Director.

6.3.4 In all cases, the member of staff responsible for making the change live will complete the relevant sections of the MiCRF which will be retained for no less than two years for reference.

7.0 COMPLIANCE

7.1 Responsibility

7.1.1 It is the responsibility of all employees to ensure that they have read, understood and abide by this standard.

7.2 Review and Monitoring

7.2.1 These processes will be reviewed and monitored by the Service Managers. Any issues around non compliance and justification in such will also be dealt with by the appropriate Line Manager.

Appendix A

Major Change Record Form

Change record form
This constitutes the formal log of a change and must be kept as a record of that change's history
Reference number:
Part A:
1. Requester name: **2. Approved by (owner):** **3. Change required to:**
Part B: (use and attach continuity sheets if required)
4. Description of change (in general not technical terms)
5. Why is the change needed?
6. What are the advantages of the change?
7. What are the recognised risks of implementing this change?
8. What are the disadvantages (if any) to the change?
9. What are the risks of not implementing the change?
Change record form (use and attach continuity sheets if required
10. What is the potential effect on the service and its users? (to include support

maintenance, licence issues, etc.)

11. Timetable for implementation

Date and time live change required:

Are users required to be 'off the system' when change is implemented?
Y/N

Do users need to be totally logged off from all systems when change is implemented Y/N

12. What resource and effort are involved in change implication?

13. In case of change failure please detail 'role back' procedure, step by step if possible

14. To be completed by Director of IM&T

Name: Date:

Approved Y/N

Further information required (please specify):

15. Implemented Y/N
16. Owner notified (date/ time)

Requester notified (date/time)

17. Documentation amended

Technical	**Y / N / not applicable**
Operating	**Y / N / not applicable**
User	**Y / N / not applicable**

Appendix B

Minor Change Record Form

This form constitutes the formal log of change and must be kept as a record of that change's history **All areas must be completed where applicable**

Person requesting change:
Date: ____________________

1. Describe change request to current system (attach additional sheet if required)			
2. Reason for change: (tick as appropriate)			
□ **Upgrade**	□ **New software**	□ **System fix**	□ **Other**
If other please specify:			

Person testing/installing change request:
Date: ____________________

3. Has upgrade, software, patch etc. been tested?	**Y/N**
Details:	
4. Was test successful? **Y/N**	
If not, what problems were encountered?	

5. If successful please give details and planned installations dates:

6. **Please details role back procedure:**

7. **Before any upgrade is installed evidence of a successful test must be produced and signed off by the following:**

Information asset owner, name:

Signature: ……………………………………….. Date: ……………………………

IM and T Manager, Name:

Signature: ……………………………………….. Date: ……………………………

Appendix C

Examples of Major and Minor Changes

Major changes can consist of the following examples:

- Replacement Servers
- Replacement Telephony System
- Adastra upgrades
- Server Upgrade (operating system, system configurations)
- Additional hardware to servers
- Changes to firewalls
- Changes to the telephony configuration

Minor changes can consist of the following examples:

- Additional network ports
- Replacement UPS
- Upgrade to Anti Virus system
- Rebooting servers
- Replacement of backup device
- Server Upgrade (Memory, Additional Hard Drives, Service Pack)
- Adastra System Update
- ACPP Change
- EMIS Web Update
- Configuration Change to Case Flow
- Amendments to DTS/EDT and DOCMAN messaging