Walton Centre

Change Control

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
06/01/2005	1.1	L Wyatt	Update to responsibility
31/03/2005	1.2	L Wyatt	Update to Trust procedure

Table of Contents

1. Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust.

The Trust acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Trust's Security Policy, Security Standards and Work Instructions Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Trust. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Trust.

This procedure outlines the standards used for the testing of software and hardware, which is used in the server farm located at the Trust.

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line managers (in scope)
Compliance	All staff and contractors (in scope)
Monitoring	Information Security Officer Information Security Auditor

3. Internal Change Approval procedures

3.1 Overview

The operational change control process covers change initiation of change, control of change, record keeping, and decision making for all aspects of change on the Trusts information systems on computer. The process have been devised to allow minimum time impact on the actual changes themselves – that is the process should not, in itself, slow down the start or pace of a change. There are two processes – one for projects and large changes (the Major Change Process) and the other for smaller changes (the Minor Change Process). Each process is described in the sections that follow.

3.2 Record Keeping And Auditing Of Changes To Systems

An audit trail will be kept. Each change will have a form which will record progress at every stage. The form will be the basis of the final implementation change control decisions process.

The Major Change Record Form (ACR) (Appendix A), and the Minor Change Record Form (ICR) (Appendix C) both form part of the documentation of this section.

3.3 Test Systems

The Test Area is an environment, a basic mirror of the Trust domain consisting off a Domain controller, Citrix Server, Exchange Server and a Client machine a client for the testing of the following;

The Test Area contains a range of equipment; various operating systems and builds are installed on the equipment. It is documented and managed under an internal change control procedure.

A label located on the front of the machine identifies each piece of equipment.

Only authorised personnel have permission to use the Test Area.

Any member of staff wishing to use the Test Area must obtain prior permission, along with approval for being stood down from their normal day-to-day tasks.

A Test Area booking form needs to be filled in and submitted to Implementation Manager (Information Security Officer) for approval.

See appendix A for Test Area booking form.

If configuration of any other changes are being made to builds then ensure that this information is supplied in the Test Area booking form along with a Change request form being submitted and signed off.

Wherever possible change & implementation work should be tested on a test system which is not a part of the live, production systems. The test systems should be as close to the live system in its configuration as possible. Changes should be tested on a test system, if possible, prior to a change implementation request being made.

3.4 Who Makes Change Control Decisions?

The decision as to whether a change is deemed to be a Major Change or a Minor Change will be taken by the Head of IT.

Major Change Control

The decision as to whether a change will be implemented on to a live system will be taken by at least three of the following:

1 The Owner of the system

2 The System Manager

3 The Head of IT

4 The Director of Finance & IT

Minor Change Control

For all minor changes the group which will give approval consists of:

1 The Head of IT;

2 The System Owner and

3 The Developer.

4. Internal Change Implementation Process

4.1 Classification

There are two different levels of change which affect the Agency's computer-based information systems, these can be 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: installing a brand new system (hardware, software etc.); replacing an existing system (hardware and/or software); upgrading operating systems or GUIs to new versions (for example Windows NT to Windows XP). It is to be used to implement whole new projects.

b) Minor changes to existing systems (**the Minor Change Implementation Process**). This process covers minor changes to systems – every change which is not covered by the Major Change Implementation Process (see section 6.5a).

The choice of process for each piece of work will be made by the Head of IT.

4.2 The Major Change Implementation Process

The process involves:

- The steps in part A of the Major Change Request From (MaCRF) will be completed by the Requester and system owner
- Part B of the MaCRF will be filled in by the Requester and the Owner and passed to the Head of IT.
- The MaCRF will be approved (or otherwise) by at least three of the officers defined above.
- The decision it will be communicated to the Requester and owner by the Head of IT.
- If the change is approved then the Head of IT will arrange for the implementation of the change.
    - Prior to implementing the change the system(s) will be safe-guarded by taking steps to provide a “fall back” position if needed [e.g. by making a back-up of the system(s) involved].
    - Once implemented the change must be monitored by the Requester, the Owner, the member of the IT department actioning the change to ensure that there are no problems. If problems occur which require invoking the “fall back” procedure on the CRF, the Head of IT will arrange this, having informed all parties involved.
- If the change is not approved their will be feedback to the requester and owner in order that they may take appropriate action (eg change their submission or abandon it etc.).
- Once implemented the relevant technical, operating & user documentation will be updated as appropriate. This is the responsibility of the Owner.
- If appropriate changes to the Business Continuity plan must be made. This will be organised by the Head of IT.

- The complete MaCRF form will be kept by the Head of IT for a period of at least 24 month as a record of the change for future reference.

4.3 The Minor Change Implementation Process

- The designation of a piece of work as a Minor Change will be made by the Head of IT.

- The Minor Change Request From (MiCRF) form should be completed by the Requester , who should give the following information:

  a) The category (whether the change is to hardware, software (including operating systems & GUIs or "other").

  b) A brief description of the change required.

  Later on the member of staff who makes the change should also note here any "intermediate" changes that needed to be done to make the change work correctly etc. – for example, if a patch is required to an operating system in order to make a new version of a web-browser work then the incorporation of that operating system patch should be noted here.

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

- Approval will be given by the Head of IT.

- In all cases, the officer responsible for making the change "live" will complete the relevant sections of the MiCRF for,m (ie "Completed", "Set Live" and "Live Date".

- The complete MiCRF form will be kept by the Head of IT for a period of at least 12 months as a record of the change for future reference.

5. Compliance

5.1 Responsibility

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

5.2 Review and Monitoring

The Walton Centre has in place routines to regularly audit compliance with this and other standards.

Appendix A: Test Area booking form

Test Area booking form

Requested By_____ **Date** _____

Machines/Build Required _____

Tests Planned _____ **Time Period** _____

Authorised By_____

Date _____

Additional Information

Appendix B: Major Change Record Form

Change record form	
This form constitutes the formal log of a change and must be kept as a record of that changes history.	
Reference number:	
Part A: **(In order for Part B to be submitted this part must be complete)**	
1. Requester name: **2. Approved by (owner):** **3. Change required to: Operating System/Application System/Hardware** (Delete as applicable)	
PART B: (In order for implementation to be authorised PART B must be complete.)	
7. Description of change to system (in general, not technical terms)	
8. Why is the change needed?	
9. What are the advantages of the change?	
10. What are the risks of implementing this change?	
11. What are the disadvantages (if any) to the change?	
12. What are the risks of NOT implementing this change?	

Change record form	
13. What is the potential effect on the service and users (include support/maintenance costs and whether approved or not; are extra licences needed?)	
14. Timetable for implementation: ▪ What date and time is change required live? ▪ Do users need to be "off the system" when the change is implemented? y/n ▪ Do they need to be totally logged off from all systems when change is implemented? y/n	
15. What resource and effort are involved in change implementation?	
16. In case of failure once the change has gone live what is the "Role back" procedure? Give full details – step by step possible.	
17. To be filled in by Head of IT: Name: Date: Approved: y/n Need more information:	
If more information needed, what information do you need?	
18. Implemented: y/n **19. Notification of implementation:** Owner (to notify users if applicable) Requester: **20. Documentation amended** Technical	y/n/not applicable

Change record form	
Operating	y/n/not applicable
User	y/n/not applicable

Appendix C: Minor Change Record Form

This form constitutes the formal log of a change and must be kept as a record of that changes history

Note all areas must be completed were applicable

Person Requesting Change: *Date:*

1. Call reference Number must be entered if associated with a helpdesk request:……

2. Describe change request to the current system. (Attach additional sheets as required.)

3. Reason for change: (Tick appropriate box)

☐ Upgrade	☐ New Software	☐ System Fix	☐ Other

If other please state

Person testing/ installing Change Request: … …… *Date*……..

4. Has the Upgrade, Software, Patch been tested ?
No. (if **No** reason for not testing)

Yes on local pc and wcnn-cit-10 (out of farm)

Yes. (If **Yes**, which server was the Upgrade, Software, Patch tested on)

5. Was the test successful Yes/No delete as appropriate

No. (if no what problems were encounted)

6. If the test was successful please give details and planned installation dates for work to be carried out .

7. Role back procedure please state the role back procedure if update does not work.

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

Approval:

Head of IT : _____ Date:_____