



# Information Management and Technology Change Control Policy

<b>Document Reference:</b>	POL061
<b>Document Status:</b>	Approved
<b>Version:</b>	V2.0

## DOCUMENT CHANGE HISTORY

Initiated by	Date	Author (s)
Head of IT	November 2012	T&T Security & Resilience Manager
Version	Date	Comments (i.e., viewed, or reviewed, amended approved by person or committee)
V1.1	November 2012	Circulated to T&T Senior Management Team for comments
V1.3	March 2017	Revised after adult- circulated to IM&T Management for comments

<b>Version</b>	<b>Date</b>	<b>Comments (i.e., viewed, or reviewed, amended approved by person or committee)</b>
V1.4	July 2017	Approved by IGG
V1.5	June 2018	Approved IGG
V2.0	April 2019	Approved by MAG

<b>Document Reference</b>	Directorate: Strategy and Sustainability
<b>Recommended at Date</b>	Information Governance Group June 2018
<b>Approved at Date</b>	Management Assurance Group April 2018
<b>Valid Until Date</b>	May 2021
<b>Equality Analysis</b>	February 2019
<b>Linked procedural documents</b>	N/A
<b>Dissemination requirements</b>	All IM&T staff and other staff as/when required/appropriate
<b>Part of Trust's publication scheme</b>	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

## Contents

<b>Paragraph</b>		<b>Page</b>
1.	Introduction	5
2.	Purpose and Scope	6
3.	Duties	7
4.	Change Process	9
5.	Dissemination & Implementation	13
6.	Process for Monitoring Compliance & Effectiveness	13
7.	Standards/Key Performance Indicators	13
8.	Associated Documents	13

## Appendices

Appendix A	Equality Impact Assessment: Executive Summary	14
Appendix B	Monitoring Table	18

## 1. Introduction

This document outlines the processes to be followed for implementing system changes or fixes within the East of England Ambulance Service NHS Trust or any alteration of critical systems and/or processes, IT hardware or software, telephony, network infrastructure and voice recording.

- To enhance communication of change, provide standards to the expectations of communications, and review processes for validating change.
- To ensure that NO changes are applied without the correct authorisation.
- To ensure that all relevant stake holders are aware of changes, and ensure any processes/procedures/documentation/asset register information that requires updating is appropriately updated and all relevant parties are aware of the change and its implications.

It is the responsibility of all staff and managers that these procedures are followed. No change authorisation = no change takes place.

Changes should be dealt with using the standard 6 D's for change management:

- Disclose
- Discuss
- Decide
- Document
- Date
- Deploy

It is the responsibility of all staff and managers that all Information Governance standards are met as part of the change control process.

The SIRO, Caldicott Guardian and relevant Information Asset Owner should be consulted as part of the change control process,

EEAST: POL061 IM&T Change Policy  
V2.0

and where necessary approve the change as part of the approval process.

## 2. Purpose & Scope

### 2.1 Purpose

This policy outlines the procedure to be followed when changes or fixes are proposed to Critical systems and/or processes, IM&T hardware or software, Telephony, Network Infrastructure and Voice recording. The purpose of this policy is:

- To ensure that no unauthorised or unscheduled changes are applied without authorisation from Senior Management
- To ensure that the Trust Performance Lead is aware and approves any changes that may affect the performance statistics
- To ensure that the Information team is aware of any changes that may affect the data warehouse, AQI standards and other reports.
- To ensure that the IT department is aware of any IT support requirements for implementation
- To ensure that the IT department is aware of changes that affect the IT out of hours support provision

### 2.2 In Scope

Change control will apply when making any system, software, hardware or other change to all systems in use in the Trust.

**Change control will also apply where:**

- Technology changes direction
- Technology replacements
- Access to data centres/server rooms for all non IT team or external contractors.

### 2.3 Out of Scope

The Change Control process does not need to be followed for business as usual (BAU) type of changes such as replacing a keyboard, phone or a routine PC swap out; nor does this process need to be followed for BAU related IT Service Desk calls. For these

BAU type changes, the standard Service Desk process will be utilized. If in doubt, contact the IT Service desk..

Example of items that would not require a change request but do require a service request

- Password reset
- General desktop support/replacing keyboards/routine PC swap out\*
- Printer/PC maintenance / swap out
- New network cable for individual PC
- A desk move for 3 or less people, for moves involving more than 3 people will require discussions with the Service Desk team leader.

\* where any hardware equipment such as PC's, E-PCR, Mobile phones etc. are swapped out, although no change process will apply asset registers and other such documentation must be updated and a record of the swap fully recorded.

All Hardware and software not listed in the Service Catalogue must go through formal IT approval process. Items must first be approved by the senior management team, then accepted as supportable by the Service Desk.

### 3. Duties

#### 3.1 Requestor

- If you are member of the IM&T directorate, raise a change request via the change control template on the service desk software (HOTH). If you are an external member to the IT directorate, please email the IT service desk and this will be logged and assigned to the appropriate member of the IT team.
- Ensure all relevant required documents are completed, including, but not limited to:-

The nature of the change

The impact of the change on the Trust, including associated IT systems or infrastructure

The risk associated with the change

The results of the testing performed for the change

The procedures in place to roll back the change in the event of an issue.

- Ensure all testing of change is completed and documented.

### **3.2 Change Advisory Board (CAB)**

The CAB will be formed of a working group which include but not limited to IM&T staff members and other key stakeholders.

Responsibilities of the CAD will be as follows:-

- Attend change meetings where appropriate
- Validate the change request, including roll back plans, test plans and impact assessments
- Assess Risks of the change
- Approve changes
- Schedule approved changes
- Formally review changes for approval and schedule changes.

### **3.4 Technical Implementation Team**

All changes require an implementation technical team, their roles are:

- To gain approval for changes (unless instructed by senior managers under the emergency change process).
- To test changes and document results in IT Service Desk software.
- To implement changes as per the steps and processes laid out in the change control documents and any relevant supporting designs or process documents.
- To report the status of the change on completion

- To report any variation to the process/change

### **3.5 Consultation and Communications with Stakeholders**

CAB will agree the responsibility for and method of the communications on a change by change basis.

### **3.6 Prioritisation of Work**

Changes are scheduled at the CAB. The CAB will review the business requirements and impact when making the assessment about any change.

### **3.7 Identification of Stakeholders**

When a change request is logged all the relevant information about impacted stakeholders are clearly identified.

## **4. Change Process**

### **4.1 Submission & Approval Process**

Before any changes can be made, a completed Change Request Form must be completed on the IT Service Desk software. Each change must include the following:-

The nature of the change

The dates of testing and live

The impact of the change on the Trust, including associated IT systems or infrastructure

The risk associated with the change

The results of the testing performed for the change

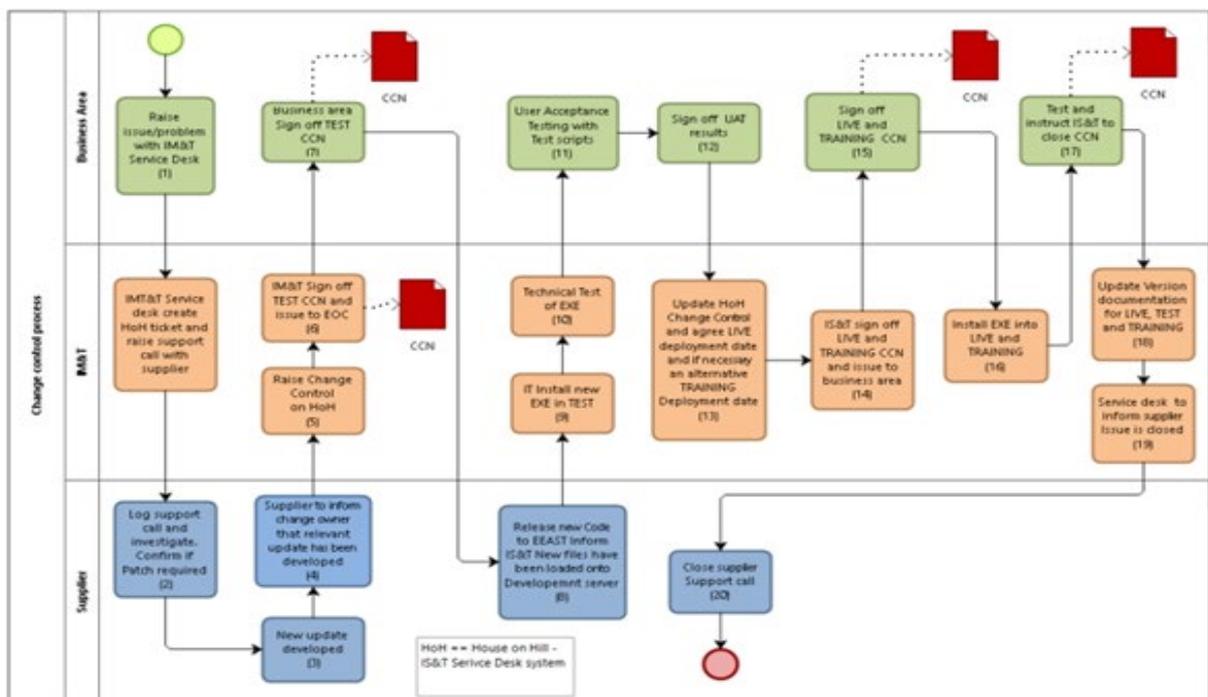
The procedures in place to roll back the change in the event of an issue.

**The notice period for changes are detailed in the next section. All changes must follow these timescales.**

CAB will review the change and discuss the change request with the department requesting the change and/or any 3rd party supplier that will be involved in the process.

The process is as follows

- Change is completed on the IT Service Desk.
- The change is then put through the appropriate change approval process, which may vary on a case by case basis. The approval levels may also vary based on the complexity and the impact of the change, however each change will go to CAB for approval.
- Once approved the change will be scheduled and the appropriate communication plan will be set out to advise the impacted users.



Powered by  
bizagi  
Monitor

## 4.2 Change Review

Each change that has been resolved will be reviewed at CAB meetings.

EEAST: POL061 IM&T Change Policy  
V2.0

#WeAreEEAST 

Should any closing statuses of previous changes highlight any impact on the current changes submitted, these new changes will be highlighted and may have to be deferred.

The review of previous changes should also check that the following has been completed:

- All relevant documentation updated
- All post change testing was successful
- All interested parties noted and advised of change status
- Change status updated

### **4.3 Change Category and Submission Lead Times**

The notification of changes must be submitted in a timely fashion.

**Standard** – Minimum 10 working days notice.

**Emergency** – something that starts as an incident/problem and results in a change/or a security risk to the trust meaning it needs to be completed before the 10 day standard change timeframe.

Lack of planning does not constitute an emergency. Emergency changes can only be approved by the Head of IM&T or the Deputy Head of IM&T (IT).

**Retrospective** – a change that has email approval (at least at IM&T manager level) prior to going ahead, this is generally to fix an issue/security risk that occurs out of hours.

**Emergency and Retrospective changes must be communicated to the Gold Commander in hours and out of hours, and where possible to other key stakeholders.**

### **4.4 Notifications**

It is the responsibility of the change owner to ensure that the appropriate level of communication is distributed to the relevant business areas. At certain phases within the change process

communication needs to be sent to the relevant business areas. These notifications need to cover but not limited to

- 1) Type of change
- 2) Date and Time
- 3) Level of change (Test, Training or Live)
- 4) Impact if known
- 5) Result of change
- 6) Next steps

When notifications are sent out communication has to always go to the IT Ops email distribution list.

In instances where changes are being raised on a business owner behalf then confirmation needs to be sought in terms of who will be releasing the communication and confirmation that these have been distributed.

#### **4.5 Change Closure**

Once a change has been initiated, authorised and implemented it will end with a closing status.

When changes have finished the status will be changed to "Implemented successfully" or "Implemented unsuccessfully" and the call resolved. The call will then be reviewed at the next CAB.

Any issues arising from finished changes will be dealt with either as an incident or further change requests as appropriate.

The change will be reviewed and feedback submitted during the next CAB meeting.

#### **4.6 Reporting**

A Change Status report will be sent to the Head of IM&T every week for review.

## **5 Dissemination and Implementation**

### **5.1 Dissemination**

This policy will be held in the document library and advertised in line with the Trust policy on dissemination of procedural documents.

It will be circulated within IM&T via the senior management team, and with relevant stakeholders as and when required.

### **5.2 Implementation**

IM&T Operational processes are currently in place in line with this policy, current legislation and best practice.

## **6 Process for Monitoring Compliance and Effectiveness**

Audits will be conducted periodically to ensure these procedures and protocols are being adhered to, failure to comply with these procedures and/or protocols will be deemed as a failure to comply with the policy and will be reported to senior management.

## **7 Standards/Key Performance Indicators**

Standards will be measured throughout the change process, both in regards to success/failure, and in adherence to process.

## **8 Associated Documents**

Information Security Policy

T&T Operational Policy

## **Appendices**

A Equality Impact Assessment: Executive Summary

B Monitoring Table

## Appendix A – Equality Impact Assessment: Executive Summary

EIA Cover Sheet	
Name of process/policy	IM&T Change Control Policy
Is the process new or existing? If existing, state policy reference	POL061
Person responsible for	IT Security & Resilience Manager
Directorate and	Strategy & Sustainability
Name of assessment lead or EIA	IT Security & Resilience Manager
Has consultation taken place?	Via email
Was consultation internal or external? (please state below):	
Internal	Head of IM&T
	Deputy Head of IM&T
	IT Infrastructure Service Delivery Manager
	IT Service Desk Service Delivery Manager

<p>The assessment is being made on:</p> <p>Please tick whether the area being assessed is new or existing.</p>	Guidelines	<input checked="" type="checkbox"/>
	Written Policy Involving staff and patients	<input type="checkbox"/>
	Strategy	<input type="checkbox"/>
	Changes Practice	<input type="checkbox"/>
	Department Changes	<input type="checkbox"/>
	Project Plan	<input type="checkbox"/>
	Action Plan	<input type="checkbox"/>
	Other (Please State)	<input type="checkbox"/>
	Training Programme	<input type="checkbox"/>

## Equality Analysis

What is the aim of the policy/procedure/practice/event?

Outlines the processes to be followed for implementing system changes or fixes to Trust systems.

Who does the Policy/Procedure/practice/event impact on? Nobody

Race	■	Religion/ Belief	■	Marriage/Civil Partnership	■
Gender	■	Disability	■	Sexual Orientation	■
Age	■	Gender re-assignment	■	Pregnancy/Maternity	■

Who is responsible for monitoring the policy/procedure/practice/event?

Change Advisory Board

What information is currently available on the impact of this policy/procedure/practice/event?

None

Do you need more guidance before you can make an assessment about this policy/procedure/practice/event?

No

Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? Yes/No

If yes please provide evidence/examples:

Race	<input checked="" type="checkbox"/>	Religion/ Belief	<input checked="" type="checkbox"/>	Marriage/Civil Partnership	<input checked="" type="checkbox"/>
Gender	<input checked="" type="checkbox"/>	Disability	<input checked="" type="checkbox"/>	Sexual Orientation	<input checked="" type="checkbox"/>
Age	<input checked="" type="checkbox"/>	Gender re-assignment	<input checked="" type="checkbox"/>	Pregnancy/Maternity	<input checked="" type="checkbox"/>

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics. Yes/No

If so please provide evidence/examples:

Race	<input type="checkbox"/>	Religion/ Belief	<input type="checkbox"/>	Marriage/Civil Partnership	<input type="checkbox"/>
Gender	<input type="checkbox"/>	Disability	<input type="checkbox"/>	Sexual Orientation	<input type="checkbox"/>
Age	<input type="checkbox"/>	Gender re-assignment	<input type="checkbox"/>	Pregnancy/Maternity	<input type="checkbox"/>

Please provide evidence:

No

**Action Plan/Plans – SMART**

Specific  
Measurable  
Achievable  
Relevant  
Time Limited  
None Required

**Evaluation Monitoring Plan/How will this be monitored**

Who  
How  
By  
Reported to

There is zero impact on any 'characteristic' therefore there is no need to monitor