East of England
Ambulance Service
NHS Trust

Digital Change Control Policy

Document Reference:	POL061
Document Status:	Approved
Version:	3.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
CIO	November 2012	IT Security & Resilience Manager
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
V 1.1	November 2012	Circulated to T&T Senior Management team for comments
V1.3	March 2017	Revised after audit - circulated to IM&T Management for comments
V1.4	July 2017	Approved by IGG
V1.5	June 2018	Approved by IGG

Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
V2.0	April 2019	Approved by MAG
V2.1		Circulated to Digital Senior Management team for comments
V2.1	March 2023	Recommended by Information Governance Group
V3.0	June 2023	Approved by Compliance and Risk Group

Document Reference	POL061 Directorate: Digital
Recommended at **Date**	Information Governance Group 16 March 2023
Approved at **Date**	Corporate Risk Group 19 June 2023
Valid Until Date	June 2025
Equality Analysis	March 2023
Linked procedural documents	None
Dissemination requirements	All staff
Part of Trust's publication scheme	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

Paragraph **Page**

Appendices

1. Introduction

This document outlines the processes to be followed for implementing system changes, security updates or bug fixes within the East of England Ambulance Service NHS Trust or any alteration of critical systems and/or processes, IT hardware or software, PowerBI reports, data scripts relating to the data warehouse and\or data lake 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 prior 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.

The IT Head of Live Services, IT Infrastructure Service Delivery Manager, Head of Digital Delivery, IT Application Service Delivery Manager, Head of Information and Data and Head of Commercial (as appropriate), along with representatives from any relevant organisational units, should be consulted as part of the change control process, and where necessary approve the change as part of the approval process.

2. Purpose

This policy outlines the procedure to be followed when changes or fixes are proposed to critical systems and/or processes, IT 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 and impacted parties

- 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 Digital department is aware of any IT support requirements for implementation

- To ensure that the Digital department is aware of changes that affect the IT out of hours support provision

3. Scope

3.1 In Scope

Change control will apply when making any system, software, hardware or other change to all systems in use in the Trust outside of BAU changes as described in section 3.2.

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.

3.2 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 Incident or Service Request calls. For these BAU type changes, the standard Service Desk process will be utilized. If in doubt, contact the IT Service desk.

Examples 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.

4. Duties

4.1 Requestor

If you are member of the Digital directorate, raise a change request via the change control template on the service desk software.

If you are an external member to the Digital directorate, email the IT service desk and this will be logged and assigned to the appropriate member of the IT team.

4.2 Change Advisory Board (CAB)

The CAB will be formed of a working group which include but not limited to Digital staff members and other key stakeholders. Responsibilities of the CAB 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.

5. Definitions

CAB – Change Advisory Board

6. Change Process

6.1 Submission & Approval Process

Before any changes can be made, a completed Change Request Form must be completed on the IT Service Desk call logging solution. 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 request 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 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.

6.2 Change Review

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

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

6.3 Change Categories 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 Live Services or or a senior manager acting on his behalf (i.e. the on-call senior manager).

Retrospective – a change that has email approval (at least at Digital senior 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.

6.4 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

- Type of chang
- Date and Time
- Level of change (Test, Training or Live)
- Impact if known
- Result of change
- Next steps

When notifications are sent out communication must include the IT Ops email distribution list.

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

6.5 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 change resolved. The change will then be reviewed at the next CAB.

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

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

6.6 Reporting

A Change Status report will be sent to the CIO and Head of Live Service every week for review.

7 Dissemination and Implementation

7.1 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 Digital via the senior management team, and with relevant stakeholders as and when required.

7.2 Implementation

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

8 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 Trust senior management.

9 Standards\Key Performance Indicators

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

10 Associated Documents

Information Security Policy

Digital Operational Policy

Appendices

A	Monitoring Table
B	Equality Impact Assessment: Executive Summary

Appendix A – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Progress of individual change requests	CAB	Service Desk system change control logs will be reviewed at each CAB meeting	Weekly at a minimum	Service Desk system change control logs	CAB will monitor directly	CAB will issue recommendations if/when relevant	CAB will review the process regularly and will amend processes or procedures if necessary
Adherence to the change process	CAB	Service Desk system change control logs	On-going monitoring will take place at least weekly	Service Desk system change control logs	CAB will monitor directly	CAB will issue recommendations if/when relevant	CAB will review the process regularly and will amend processes or procedures if necessary

Appendix B – Equality Impact Assessment

<table>
<tr><th colspan="2">EIA Cover Sheet</th></tr>
<tr><td>Name of process/policy</td><td>Digital Change Control Policy</td></tr>
<tr><td>Is the process new or existing? If existing, state policy reference number</td><td>POL061</td></tr>
<tr><td>Person responsible for process/policy</td><td>Digital Security & Resilience Manager</td></tr>
<tr><td>Directorate and department/section</td><td>Digital</td></tr>
<tr><td>Name of assessment lead or EIA assessment team members</td><td>Chief Digital Information Officer</td></tr>
<tr><td>Has consultation taken place?
Was consultation internal or external? (please state below):</td><td>Internal</td></tr>
<tr><td>The assessment is being made on:</td><td>
<table>
<tr><td>Guidelines</td><td></td></tr>
<tr><td>Written policy involving staff and patients</td><td>X</td></tr>
<tr><td>Strategy</td><td></td></tr>
<tr><td>Changes in practice</td><td></td></tr>
<tr><td>Department changes</td><td></td></tr>
<tr><td>Project plan</td><td></td></tr>
<tr><td>Action plan</td><td></td></tr>
<tr><td colspan="2">Other (please state)
Training programme.</td></tr>
</table>
</td></tr>
</table>

Equality Analysis

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

To provide instruction and guidance to be followed for implementing system changes or fixes within the Digital environment of the Trust

Who does the policy/procedure/practice/event impact on?

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?

Digital Security & Resilience Manager

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? Yes/No

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	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□

Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Please provide evidence:

This policy does not have any impact on any protected characteristics

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	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Please provide evidence:

This policy does not have any impact on any protected characteristics

Action Plan/Plans - SMART

Specific

Measurable

Achievable

Relevant

Time Limited

Evaluation Monitoring Plan/how will this be monitored?

There is zero impact on any "characteristic" therefore there is no need to monitor.
Who

How

By

Reported to