South East Coast Ambulance Service NHS
NHS Foundation Trust

IT Change Management Policy

Contents

1 Statement of Aims and Objectives

1.1. South East Coast Ambulance Service NHS Foundation Trust (the Trust) increasingly relies upon Information Technology services in order to deliver patient care. The interdependencies between the elements of the IT infrastructure are complex and the results of changes made to one element may have serious consequences for the others.

1.2. The uncontrolled implementation of changes to the Trust's IT systems and Infrastructure utilised to perform its core business functions presents a significant risk to the Trust. Changing system requirements, resolution of known issues, implementation of new services and routine maintenance all require appropriate Change Management.

1.3. Change Management ensures the stability of systems and IT infrastructure by; the identification and mitigation of associated implementation risks and the minimisation of disruption to the Trust's operations, consequently improving the services and service levels provided to the organisation.

1.4. Change management also acts as an enabler by supporting and facilitating the implementation and delivery of projects with IT dependencies with IT dependencies from across the Trust.

1.5. The Trust has adopted a change management policy following the industry best-practice standards of ITIL – the Information Technology Infrastructure Library, with a risk-based approach.

1.6. This policy outlines the IT Change Management procedure, including its roles and accountabilities. The policy covers all IT based systems or services regardless of department. Breaches of policy will be recorded as a Datix Incident.

2 Definitions

2.1. This policy includes all IT related infrastructure, applications, or systems upon which any department or service within the Trust relies upon in order to perform their normal duties.

2.2. A change can be defined as the addition, modification or removal of any authorised, or supported service or service component that could affect IT services. However, this will exclude business as usual and day to day administrative activity along with returning systems or services to their original working state.

2.3. The IT department is the custodian of IT Change Management, but Information Technology is a function which spans the entire organisation, and any area could introduce IT related change.

2.4. All changes to any of the Trust's IT related systems are required to follow the established “IT Change Management Procedure”, to ensure the mitigation of associated risks and minimise disruption to business-critical services.

3 Change Types

3.1. All changes as defined above will be considered as Normal changes unless one of the following exceptions apply:

3.2. **Emergency Change:** An Emergency change is directly related to a high priority incident, in or out of hours, and that must be implemented to restore or maintain service. Without this there would be the potential for:

- a significant adverse impact on patient safety or the delivery of patient care;
- or a significant financial loss, significant reputational impact and/or disruption to the Trust or a Trust Service Recipient.

3.3. **Expedited Change:** An Expedited change would only be considered in response to an urgent IT or wider business requirement during normal working hours - examples of which are:

3.4. Cyber Security as dictated by 3rd party organisations such as NHS Digital.
Trust directive where a named senior manager (band 8 or above) accepts accountability for risks associated implementation outside of normal CAB process.

3.5. **Major Change:** A Major change carries a high risk to the Trust, its staff or its services.

3.6. **Standard Change:** Standard changes are pre-approved changes that are considered low risk, are performed frequently, and follow a documented process. Standard changes will only be sighted at CAB for final approval.

3.7. **Minor Change:** A Minor change is a change type that does not require a significant amount of preparation and planning, considered to be no risk or very low-risk, and will not have an end-user impact.

4 Responsibilities

4.1. The **Senior Information Risk Owner** (SIRO) takes ownership of the organisation risks associated to Information Assets and acts as an advocate for information risks to the Board, providing advice to the Accounting Officer. The SIRO is responsible to the Board for Information Asset Risk and the corresponding information asset policies, management, and governance. Information Asset changes, which in the context of this policy may be subject to SIRO interest are as follows:

- Changes to the availability of information outside of the organisation.
- Changes which pose significant risk to the availability of information within the organisation.
- Fundamental changes to the logical or physical security of information assets.
- Fundamental changes to the business continuity capability, or changes which pose significant risk to the organisation's ability to invoke the disaster recovery of information assets.

4.2. The **Associate Director for IT** is responsible for the provision of formal assurance concerning the Information Assets managed by the IT department, directly or via subcontractors.

4.3. The **Change Requester** is the individual responsible for preparing and submitting an RFC.

4.4. This person will support the collection of the necessary business information and engaging with the concerned stakeholders before the change request is submitted and ensuring they follow the IT Change Management Procedure and related best practices.

4.5. The **IT Head of Infrastructure/Head of IT Service Delivery/Head of Critical Systems/IT Data Manager** are responsible for the oversight of the actual implementation of changes and any subsequent incidents and problems associated, particularly within the production environment.

4.6. The **Head of Estates** responsible for existing building services such as power and air conditioning upon which IT infrastructure and services is reliant and will be required to submit RFC for maintenance events.

4.7. The **IT Change Manager** is accountable for the overall process operation, including monitoring the process to identify and rectify issues and remove bottlenecks. The Change Manager also chairs Change Approval Board (CAB) meetings, manages CAB approvals, and performs the tasks related to updating the RFC records, categorisation, and reporting of change metrics.

4.8. The IT Change Manager is responsible for ensuring that all Trust staff are aware of the IT Change Management Policy and Procedures and that the IT Change Management Procedure is followed.

4.9. The **Change Advisory Board** (CAB) reviews all non-minor changes in regard to their planned implementation (as detailed in the IT Change Management Procedure) and provides a rigorous assessment of the proposed change. Minor changes will be retrospectively reviewed during CAB for appropriateness.

4.10. The CAB evaluates the business and technical risks, the compliance with existing policies and procedures, the impact on the live environment, the benefits associated with the RFC amongst other criteria and the resource allocation for the change.

4.11. The CAB then provides assurance to the Associate Director of IT that a change is either suitable to progress with impacts to business services minimised or justified in being delayed or cancelled.

4.12. Based on the aforementioned assessment, CAB members will discuss any commented change and unanimously advise the IT Change Manager whether the change should be approved, rejected or ask for specific modifications to the proposed plans to meet organisational requirements before resubmission.

- The fixed membership of the CAB includes:
- IT Supplier Manager (IT Change Manager)
- Head of Infrastructure & Networks
- Head of Critical Systems
- Head of IT Service Delivery
- IT Data Manager

4.13. To conduct and complete a non-technical discussion, the CAB meeting will be limited to the fixed members and in the event of fixed members being unavailable, their respective delegate can make a decision on their behalf. The members required to make a CAB decision are subject to the discretion of the IT Change Manager, and there is a minimum quorum of at least three members.

4.14. In the unlikely event that CAB does not meet quorum, business critical and/or reputational changes that have been pre-approved and scheduled before the next CAB can be authorised to proceed by the Associate Director of IT.

4.15. The IT Change Manager will co-ordinate when the CAB will meet and the agenda will be automatically distributed prior to the meeting. All changes required for the following week will need to be submitted and fully approved by close of play three business ahead of CAB.

5 Service Stakeholders

5.1. For each service within the scope of this process, the key business stakeholders should be identified with help from the Change Requester. This allows those stakeholders the opportunity to provide an assessment of any risks or impact from their perspective, and any other relevant feedback. The process should ensure these stakeholders are notified of any changes which may affect key services the Trust provides (e.g., system outage, service disruptions, hardware/software upgrades, etc.)

6 Change Management Procedure

6.1. The IT Change Management Procedure provides assurance that standardised methods and procedures are used for efficient and prompt handling of all Changes. A formal process of recording, assessment, authorisation, scheduling, and comprehensive communications is in place for all changes. This is done to minimise the impact of Change-related incidents upon service quality, and consequently to improve the day-to-day operations of the IT services that the Trust provides.

6.2. Change Management also aims to provide the Trust with the ability to rapidly adapt to business requirements as they change, increasing its ability to ensure a customer focused operation is maintained at all times, while minimising disruption to key IT systems and services.

7 Risk Management

7.1. The Trust's approach to Change Management relies on a Risk and Impact Management based approach. To comply with that, all changes must be properly documented as per the IT Change Management Procedure in line with the Trust Risk Management and Procedure. Risk Assessment Matrix – see. 7.2

Risk Assessment Matrix – Level of Risk

		Consequence				
		Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Likelihood	Rare (1)	1	2	3	4	5
	Unlikely (2)	2	4	6	8	10
	Possible (3)	3	6	9	12	15
	Likely (4)	4	8	12	16	20
	Certain (5)	5	10	15	20	25

Score	Descriptor	Description
1	Rare	Not expected to happen again
2	Unlikely	May happen but in exceptional or unusual circumstances
3	Possible	The event may re-occur occasionally,
4	Likely	The event will probably re-occur
5	Certain	The event is likely to re-occur on many occasions

Qualitative Measures of Likelihood and Risk Assessment Matrix

Score	Risk Preventative Measures to be Taken or Planned
Low Risk 1-6	Manage by routine procedure. Implement any action that will eliminate the risk of the incident /risk occurring
Medium Risk 8-15	Senior Management action needed. The responsible Director must be aware and Lead Manager must devise and implement an action plan to control, reduce or eliminate the risk. Risk must be inputted onto the Corporate Risk Register.
High Risk 16-25	Immediate action required. The Risk Managers and Executive Management Team must be made aware and are responsible for ensuring an investigation and action plan is commenced immediately to reduce, control or eliminate the risk. The risk must be entered onto the Corporate Risk Register

8 Audit and Review

8.1. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

8.2. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

8.3. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

8.4. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies**.**

9 References

9.1. **IT:** is an abbreviation for Information Technology and is used as a collective term to describe all systems and services associated with computers and data networks.

9.2. **ITIL:** The IT Infrastructure Library is a collection of internationally recognised best-practices for delivering IT Services, covering all aspects of service provision, quality assurance, and providing a framework which allows customisation of internal processes.

9.3. **Change Management:** One discipline within the ITIL process framework which has the aim of ensuring appropriate controls are placed around changes to IT Systems and Services to mitigate risks, ensure stability, provide responsiveness to changing organisational requirements and minimise service disruption.

9.4. **CAB:** The Change Advisory Board. As can be inferred from the name, this body has no governance role, but is tasked with advising the IT Change Manager and Business Stakeholder of the perceived impact of a requested change. This body is made up of fixed members representing all major core IT Services and teams. The CAB incorporates other required stakeholders depending on the nature of the RFC being assessed.

9.5. **RFC:** Request for Change – is an electronic form which contains all the required information for the process to be started, initiating the Change Management process.

9.6. **GDPR:** General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018

10 Financial Checkpoint

10.1. This document has been confirmed by Finance to have no unbudgeted financial implications.