|  |
| --- |
| Business Requirements Document  Living Donation Project  Requirements to move to transition state one in digitising Living Donation |
| NHS Blood and Transplant |

|  |
| --- |
| Author: Matthew Thorogood  Version: 0.1 Issue Date: 4th December 2020 |

|  |
| --- |
| Table of Contents |
| [1 Summary 3](#_Toc60853654)  [1.1 Purpose of Document 3](#_Toc60853655)  [1.2 Glossary 3](#_Toc60853656)  [1.3 Objectives 3](#_Toc60853657)  [1.4 Scope and Limitations 3](#_Toc60853658)  [1.5 Benefits - TBC 3](#_Toc60853659)  [2 Current Business Situation 4](#_Toc60853660)  [3 Desired Business Situation 4](#_Toc60853661)  [3.1 Context Diagram 4](#_Toc60853662)  [4 Business Requirements 5](#_Toc60853663)  [4.1 High Level System (presented as a use case) 5](#_Toc60853664)  [4.2 Use Case Descriptor 6](#_Toc60853665)  [4.3 Functional Requirements (Replaced by user stories on scrums if relevant) 6](#_Toc60853666)  [4.4 Non-Functional Requirements 7](#_Toc60853667)  [4.5 Reporting Requirements 7](#_Toc60853668)  [5 Data 7](#_Toc60853669)  [6 Appendices 8](#_Toc60853670)  [6.1 MoSCoW Definitions 8](#_Toc60853671)  [7 Appendix B – Non-Functional Requirements 10](#_Toc60853672)  [8 Appendix C – Document Reference 22](#_Toc60853673)  [8.1 DOCUMENT LOCATION 22](#_Toc60853674)  Do not remove |

© NHS Blood and Transplant 2021.

Other than for the sole purpose of evaluating this , no part of this material may be reproduced or transmitted in any form, or by any means, electronic, mechanical, photocopied, recorded or otherwise or stored in any retrieval system of any nature without the written permission of NHSBT.

NHS Blood and Transplant, 2nd floor, 65 New Street, Birmingham B2 4DU

Telephone: 01923 486800 Fax: 01923 486801

Registered Office: Oak House, Reeds Crescent, Watford, Hertfordshire, WD24 4QN. Registered in England.

# Summary

## Purpose of Document

* The purpose of this document is to state the business requirements for linking the NHS-BT to the Transplant Risk and Consent tool, hosted on third party infrastructure.
* This document will form the basis for the architectural blueprint outlining the high-level design decisions made by the Solutions Architect.

## Glossary

| Acronym / Term | Definition |
| --- | --- |
| TRAC | Transplant Risk and Consent |

## Objectives

* This project aims to link NHS-BT websites to third party (Winton Centre) hosted architecture, enabling clinicians and their patients to use the Winton Centre TRAC tool
* The BRS aims to identify the user requirements for linking to this third-party architecture

## Scope and Limitations

* This BRS is for the TRAC ‘Tactical’ solution only. This includes, and is limited to, linking to the TRAC tools as designed by the Winton centre.
* There is appetite to have a longer term ‘Strategic’ solution, which includes hosting the TRAC tool internally and using the platform created to create TRAC solutions for other organs involved with transplants. This is beyond the scope of this BRS. However, this BRS will link to an addendum explaining the user-centred research which has taken place and must form the basis for user requirements for this strategic solution.

## Benefits - TBC

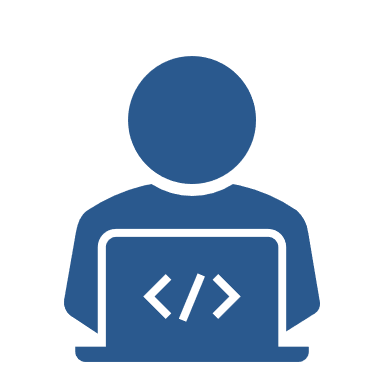
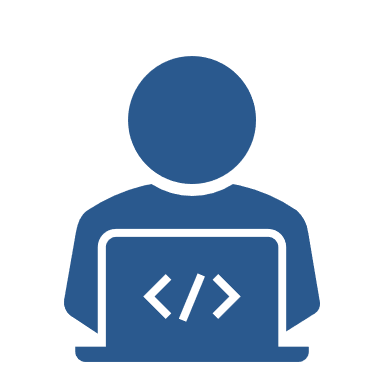
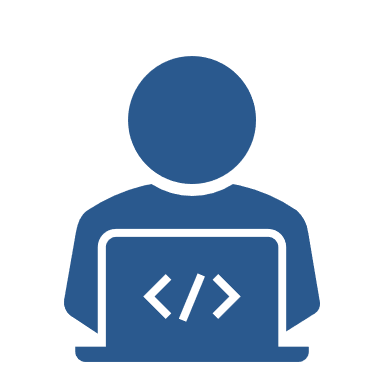
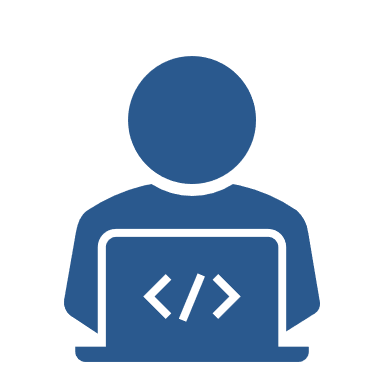
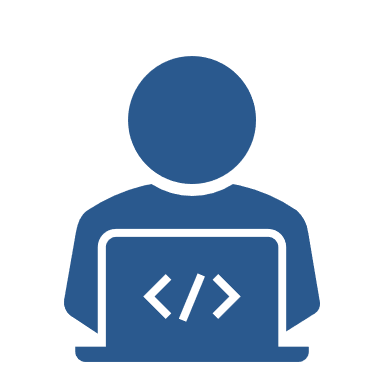
|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Current Business Situation

As there is no current TRAC tool, and it represents a new tool which can be used during consultations, there is no current business situation.

# Desired Business Situation

## Context Diagram

Logo, icon

Description automatically generatedA picture containing furniture, building, table, window

Description generated with very high confidence

***NHSBT***

***Online – central site***

***Clinician***

***NHSBT***

***Statistical Team***

***Winton Centre***

***TRAC***

***Transplant Statistical Data***

***Linked Website***

***Patient***

# 

|  |
| --- |
| Scope |
| 0- Transplants Statistical Data is sent to the Winton Centre and uploaded in the TRAC Tool.  1- Patient and Clinician discuss pro and cons of undertaking Transplant surgery. NHSBT site offers some information on transplant.  2- On NHSBT website there is a link to the Winton Centre TRAC Tool. Clinician uses the TRAC tool together with the patient to explain pro, cons of transplant and statistical evidence of what can happen. |

# Business Requirements

Requirements in this document are documented as high-level system requirements (presented as a use case diagram) and functional requirements.

## 4.1 High Level System (presented as a use case)



## 4.2 Use Case Descriptor

The following Use Case Descriptor is to be used in conjunction with the Use Case Diagram:

|  |  |
| --- | --- |
| **Use Case** | Access Winton Centre TRAC Tool |
| **Unique Id** | UC001 |
| **Scope** | Accessing the Winton centre website |
| **Primary Actor (s)** | Clinician (with patient) |
| **Pre-Conditions** | Ability to access webpages |
| **Trigger / Event** | Clinician has consultation with patient and wants to provide them statistical information based on their input factors |
| **Success guarantee** | Clinician accesses Winton Centre TRAC Tool |
| **Minimal guarantee** |  |
| **Associated Non-functional requirements** | See NFRs |
| **Priority (M, S, C, W)** | M |
| **Stake holder (s)** |  |
| **Main Success scenario:** | |
| 1 – Clinician wants to visit TRAC tool with patient  2 – Clinician accesses NHS-BT webpage  3 – Clinician follows link to TRAC tool | |
| **Extensions (Alternative paths)** | |
|  | |

|  |  |
| --- | --- |
| **Use Case** | Access Outcomes |
| **Unique Id** | UC002 |
| **Scope** | User submits inputs and receives statistical outcomes |
| **Primary Actor (s)** | Clinician (with patient) |
| **Pre-Conditions** | Accessed Winton Centre TRAC |
| **Trigger / Event** | Clinician has consultation with patient and wants to provide them statistical information based on their input factors; clinician has followed link from NHS-BT |
| **Success guarantee** | Outcomes are provided to patient which can be printed |
| **Minimal guarantee** | Outcomes provided to patient |
| **Associated Non-functional requirements** | See NFRs |
| **Priority (M, S, C, W)** | M |
| **Stake holder (s)** |  |
| **Main Success scenario:** | |
| 1 – Patient and clinician input relevant input factors  2 – Information submitted  3 – Statistical outcomes are returned in consultation | |
| **Extensions (Alternative paths)** | |
|  | |

## 4.3 Functional Requirements (Replaced by user stories on scrums if relevant)



## 4.4 Non-Functional Requirements

See Appendix B for NHS-BT general Non-Functional Requirements associated with NHS-BT website.

Specific relevant NFRs of the TRAC tool itself are:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Unique Identifier** | **Use Case ref** | **Description** | **Priority** | **Acceptance Criteria** |
| NF1 | Response Time | The TRAC tool should return the outcomes associated with the input factors within 10 milliseconds | S | Refresh rate <10 milliseconds |
| NF2 | Unique Visitors | The TRAC tool needs to be able to host up to 30,000 sessions per month (the number of visitors to NHS Predict) | M | Number of monthly sessions up to 30,000 |
| NF3 | Supported Browsers | The tool should work on browsers from Internet Explorer onwards | M | Tool works on IE11+ |

## 4.5 Reporting Requirements

To be reviewed as part of the detailed requirements:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Unique Identifier** | **Actor** | **Source** | **Description** | **Priority** | **Owner** | **Acceptance Criteria** |
| R0001 | TRAC |  | Session Counts – to know the useage of the tool | M | Winton Centre | Report of tool usage each month |
| R0002 | TRAC |  | User information (where from etc) | C | Winton Centre | Report of tool users each month |

# Data

Included w/ technical blueprint

# Appendices

Insert any relevant references

* E.g. Relevant ToR or work mandate

## MoSCoW Definitions

The following definitions have been used when prioritising the requirements

|  |  |  |
| --- | --- | --- |
| M | Must have | Must have (mandatory for the first increment of a solution, essential) |
| S | Should have | Should have (mandatory, but can be deferred for a short period until the second increment) |
| C | Could have | Could have (desirable but may not be implemented due to time and budget) |
| W | Want to have | Want to have, but won’t have this time (identified as a requirement, but will be deferred to a later stage, e.g. if the business is not ready, or the requirement needs more consideration) |

The following standards may be consulted when writing and reviewing requirements:

* Good Automated Manufacturing Practice (GAMP5)
* EU Good Manufacturing Practice Vol. 4

<http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm>

as expressed in the Blood Safety and Quality Regulations 2007 no. 604 (as amended) [Enforced by the Medicines and Healthcare products Regulatory Agency (MHRA)

<https://www.gov.uk/guidance/blood-authorisations-and-safety-reporting>

The following sections may be particularly relevant:

* Annex 11 – Computerised Systems

<http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf>

* Annex 15 – Qualification and Validation

http://ec.europa.eu/health/files/eudralex/vol-4/2015-10\_annex15.pdf

Other guidelines, accrediting bodies and regulations relevant to NHSBT that may need to be considered include

* The Human Tissue Act (2004) [Enforced by the Human Tissue Authority (HTA)] <http://www.legislation.gov.uk/ukpga/2004/30/contents>, amended by the Human Transplantation Wales Act 2013 <http://www.legislation.gov.uk/anaw/2013/5/pdfs/anaw_20130005_en.pdf>
* The Human Tissue Scotland Act, 2006 http://www.legislation.gov.uk/asp/2006/4/pdfs/asp\_20060004\_en.pdf
* EU Tissue and Cells Directive enforced in the UK in Human Tissue (Quality and Safety for Human Application) Regulations 2007 [Enforced by the Human Tissue Authority (HTA)] <http://www.legislation.gov.uk/uksi/2007/1523/contents/made>
* The Quality and Safety of Organs Intended for Transplant Regulations 2012 [Enforced by the Human Tissue Authority] <http://www.legislation.gov.uk/uksi/2012/1501/pdfs/uksi_20121501_en.pdf>
* Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga\_19980029\_en.pdf
* Clinical Pathology Accreditation (CPA) <http://www.cpa-uk.co.uk/>
* European Federation of Immunogenetic (EFI) <http://www.efiweb.eu/>
* Foundation for the Accreditation of Cellular Therapy (FACT-NetCord) <http://www.factwebsite.org/>
* Joint Accreditation Committee ISCT-EBMT (JACIE) accreditation for Cell Processing <http://www.jacie.org/>
* British Committee for Standards in Haematology (BCSH) <http://www.bcshguidelines.com/>

The following are not accessible on the Internet; however, copies are kept by QA:

* BS EN ISO 9001:2008 Quality management systems — Requirements
* BS EN ISO 13485:2003 Medical devices — Quality management systems
* ISO 22301 - Societal security -- Business continuity management systems
* ISO/IEC 27001:2005 Information Security management systems — Requirements
* ISO 22301:2012 Societal Security: Business Continuity

This is not an exhaustive list, and items on this list may be superseded over time. Guidance on use and relevance of standards, guidelines and regulations may be sought from Quality Assurance.

# Appendix B – Non-Functional Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requirement** | **Priority** | **Responsibility** | **Acceptance Criteria** | **Owner** |
| Any access to system data records containing Personal Identifiable Data and Confidential information (read or write) must be captured and retained as part of an audit log. | MUST | NHSBT | User access to system is visible and reportable | Head of Information Security |
| Date, time and individual login MUST be captured as part of log. |
| All changes to system records must be captured and attributed to an individual user login and retained as part of an audit log. | MUST | NHSBT | 1. All changes to records must be attributed to an individual login. | Head of Information Security |
| 2. Date and time of changes made must also be captured. |
| All changes to system workflows should be attributable to an individual login and be retained as part of the audit log. | MUST | NHSBT | 1. All changes made must be visible | Head of Information Security |
| 2. Individual login visible |
| 3. Time and date stamp visible |
| Once data is written to an Audit Log this MUST be accessible as Read-Only. | MUST | NHSBT | 1. Audit Log accessible | Head of Information Security |
| 2. Data is visible |
| 3. No changes can be made to the visible data |
| Audit logs MUST only be accessible to users with approved privileges. | MUST | NHSBT | 1. System administrator can log in and view the log | Head of Information Security |
| 2. Other users when logged in cannot view the log |
| 3. Logs must be stored in a access controlled environment. |
| All audit logs must be retained for a x years as defined in the retention policy | MUST | NHSBT | 1. Clear retention policy timescale adherence | Head of Data Management |
|  |
| A cloud solution should provide a mechanism for audit data to be downloaded for analysis. | SHOULD | NHSBT | 1. Audit data stored in cloud | Head of Information Security |
| 2. Audit data downloaded securely |
| 3. Once data is downloaded it is formatted as prior to download |
| 4. it is possible to manipulate the data in excel |
| 5. Individual login used to download is recorded in audit log |
| The solution must ensure that any changes made to: | MUST | NHSBT | 1. Any changes to data are attributed to an individual login in | Head of Information Security |
| -infrastructure | 2. Any changes to infrastructure are attributed to an individual login in |
| -applications | 3. Any changes to data are attributed to an individual login in |
| -data | 4. This above information is viewable in the audit log |
| in all environments is attributable to an individual. |  |
| Audit data must be held separately from operational data and be signed to prevent unauthorised changes | MUST | NHSBT | Technical specification approved by responsible person | Head of Data Management |
| The system must ensure NHSBT can retain records needed for full traceability for at least 30 years from the point of receipt of the blood or blood component | MUST | NHSBT | Process approved by legally responsible person | Head of Data Management |
| Blood establishments must retain specified information regarding donors, establishment activity and testing of donated blood for a minimum of 15 years . | MUST | NHSBT | Process approved by legally responsible person | Head of Data Management |
| All system records should be versioned so the time, date, system and author can be identified | Should | NHSBT | An agreed documented versioning standard used throughout NHSBT | Head of Data Management |
| The solution must be able to accommodate "x" transactions per second with a response time of "x" per transaction. The solution must be able to accommodate "x" transactions per day with a response time of "x" per second. | MUST | Supplier | x concurrent transactions are accommodated per second with a response time of x. | Head of Testing |
| The solution must be able to accommodate "x" concurrent users, and a maximum total number of "x" users. | MUST | Supplier |  |  |
| Subcontracted elements of the service must comply with NHSBT agreed NFRs and Policies. | MUST | NHSBT | Audited tests and policy submission and review. | Head of Information Security |
| Data must be categorised and maintained in line with NHSBT Information Governance Policy. | MUST | NHSBT | Process approved by legally responsible person | Head of Information Governance |
| The system must protect the integrity, confidentially and security of data inline with NHSBT Information Governance and security policy. | MUST | NHSBT | Technical specification approved by responsible person | Head of Information Security |
| The provider must have established processes in place for the export of NHSBT data if either party terminate the service contract | MUST | NHSBT | Technical specification to be provided before contract award | Head of Data Management |
|  |
| Where data is recorded concurrently by more than one system the data owner must define which system generates and retains the primary record. | MUST | NHSBT | Approved process for the identification of record with primacy | Head of Data Management |  |
| All medical records should be maintained in compliance with AoMRC medical record keeping standards | SHOULD | NHSBT | Signed off by NHSBT Approved Person (AoMRC Compliance) | Head of Information Governance |  |
| Any records management system must use metadata in compliance with: The Cabinet Office e-Government Metadata Standard v3.1 2006 | MUST | NHSBT | Signed off by NHSBT Approved Person (AoMRC Compliance) | Head of Information Governance |  |
| Records must be stored using an agreed classification system | MUST | NHSBT | A record classification system is defined | Head of Information Governance |  |
| Any complaint records recorded in the system should be stored separately from any relevant medical record however be traceable to the medical record where relevant. | SHOULD | NHSBT | 1. The system holds complaint records in a separate area that is not accessible by those that do not need to view | Head of Information Governance |  |
| 2. The medical record does not have any association with the complaint record |  |
| The system must support an auditable Freedom of Information process. | MUST | NHSBT | 1. It must be possible to retrieve data that would support any FOI request | Head of Information Governance |  |
| The solution must meet NHSBT’s requirements to maintain the Availability, Confidentiality and Integrity of patient, donor and organisational data at all times. | MUST | Head of Data Management | 1. Signed agreement between NHSBT and Supplier. | Head of Information Security & Information Governance |  |
| 2. Audited tests and policy submission and review. |  |
| The solution must provide access to audit meta-data which must cover as a minimum, the number of modifications, deletions, access, views of relevant data. | MUST | Supplier | 1. All modifications of data are provided via meta data which are accessible by authorised users | Head of Information Security |  |
| 2. All deletions of data are provided via meta data which are accessible by authorised users |  |
| 3. All access of data is provided via meta data which is accessible by authorised users |  |
| NHSBT must comply with the following | MUST | NHSBT | Compliance with as directed by a Responsible Person | Quality Systems Development Manager |  |
| 1. General Data Protection Regulation 2016/679 |  |
| 2. Human Rights Act 1998 |  |
| 3. The Freedom of Information Act 2000 |  |
| 4. Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998) |  |
| 5. Computer Misuse Act 1990 |  |
| 6. Copyright, Designs and Patents Act 1988 |  |
| 7. Crime and Disorder Act 1998 |  |
| 8. Electronic Communications Act 2000 |  |
| 9. Regulation and Investigatory Power Act 2000 (and lawful business Practice Regulations 2001) |  |
| 10. Compliance with Communications Act 2003 |  |
| 11. Common Law Duty of Confidentiality |  |
| 12. The Caldicott Principles |  |
| 13. Compliance with The Blood Safety and Quality Regulations 2005 (amended by the Blood Safety and Quality (Amendment) Regulations 2005 and the Blood Safety and Quality (Amendment) (No. 2) Regulations 2005) |  |
| 14. The NHS Operating Framework 2012/13 |  |
| 15. The Human Tissue Act (2004) and subsequent amendments |  |
| 16. The Tissue Quality and Safety Regulations (2007) and subsequent amendments |  |
| NHSBT and its suppliers must comply with all audit requests from the MHRA (The Medicines and Healthcare products Regulatory Agency) | MUST | NHSBT | Comply with all audits requests. | Quality Systems Development Manager |  |
| Electronic records may be signed electronically. Electronic signatures must be permanently linked to their respective record and include the time and date that they were applied | MUST | NHSBT | 1. The system is able to accommodate electronic signing. | Quality Systems Development Manager |  |
| 2. Once electronically signed the record displays time and date stamp of signature |  |
| Execution of the backup process must not impact system availability or performance. | MUST | Supplier | 1. As the back up is being undertaken the system availability and performance must be the same as before the back up | Head of Service Management |  |
| A solution must have a defined and approved backup cycle and schedule. | MUST | NHSBT | 1. A clear back up cycle must be included in the technical documentation | Head of Service Management |  |
| 2. The technical documentation must specify frequency and type of backups (full, differential, incremental), where they will be stored, how they are stored e.g. encrypted at rest), how long they should be retained. |  |
| Backups must be regularly tested to ensure they are functional. | MUST | NHSBT | NHSBT Approved Procedure | Head of Service Management |  |
| *(we may need to write this).* |  |
| The solution MUST support [the peak times of usage and maximum transactional volumes] without a reduction in response time or functionality. | MUST | NHSBT | 1. At peak usage time the functionality must not be affected via a reduced response time | Architecture & Design |  |
| The solution MUST support the specified number of users at peak times of usage of the system | MUST | NHSBT | Testing by NHSBT | Architecture & Design |  |
| The solution MUST allow a user to login to the service within "nn" seconds of entering user credentials. | MUST | NHSBT | 1. A user enters their unique details | Head of Business Services |  |
| 2. The user has access to system functionality within 10 seconds |  |
| The solution must present a login screen within "nn" seconds of the user requesting to login. | MUST | NHSBT | 1. A user requests login | Head of Business Services |  |
| 2. A log in screen is presented within 2 seconds |  |
| Any Application/Code/Transaction level application monitoring in the background must not impact the user experience of solution | MUST | NHSBT | Testing by NHSBT | Architecture & Design |  |
| The solution must be available on a 24/7 basis (365/366 days a year, and achieve an availability rate of "x"% | MUST | NHSBT | 1, Availability of the system to be trackable | Head of Business Services |  |
| Any system transactions that support the Manufacturing process ( i.e. request/response transactions) should be completed in less than one second | SHOULD | NHSBT | 1. All system transactions are completed in less than one second | Architecture & Design |  |
| The solution must adhere to Digital's best practice data security guides at https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care | MUST | Supplier | Supplier specification and testing | Head of Information Security |  |
| Access permissions for application data must only be changed by the system’s data administrator. User access levels have been defined as: | MUST |  | 1. All access roles cannot change access permissions for other users | Head of Information Security |  |
| - Role x/ Group 1 | 2. Users can access the functionality defined in requirement |  |
| - Role x Group 2 |  |  |
| The solution should have Intrusion prevention / detection systems in place to protect NHSBT Data and Systems. | SHOULD | Supplier | 1. Penetration tests | Head of Information Security |  |
| The solution must ensure communications are routed via a firewall when traversing a security boundary. | MUST | Supplier | Audited tests and policy submission and review. | Head of Information Security |  |
| The solution must ensure there is logical separation between production and non-production environments. | MUST | Supplier | 1. Signed agreement between NHSBT and Supplier | Head of Information Security |  |
| 2. System testing |  |
| The solution must ensure that NHSBT’s network communications are logically separated from other clients. | MUST | Supplier | Audited tests and policy submission and review. | Head of Information Security |  |
| Any cloud solution must have embeded data anti-theft mechanisms to ensure the safeguarding of data | MUST | Supplier | Audited tests and policy submission and review. | Head of Information Security |  |
| The cloud solution MUST use end to end encryption to protect data whilst it is in transit or at rest. | MUST | NHSBT | 1. Audited testing | Head of Information Security |  |
| 2. Policy submission and review. |  |
| The solution must not contain back door accounts, passwords or hard coded passwords that may allow an attacker to compromise the solution’s security | MUST | Supplier | Supplier signed commitment | Head of Information Security |  |
| The solution should ensure that where the use of federated authentication is not available, 2 factor authentication should be used. | SHOULD | Supplier |  | Head of Information Security |  |
| All user accounts for the solution must be able to support a provisioning and approval process administered by NHSBT staff | MUST | NHSBT | 1. To request a user account the solution must prompt for approval from an authorised user | Head of Information Security |  |
| The solution must ensure that all user accounts are requested to change passwords on a regular basis, the time period to be definable by NHSBT | MUST | NHSBT | 1. After x amount of time a user is prompted to change their password | Head of Information Security |  |
| The solution should automatically tailor menu systems for users based on security level. (Only seeing the functions applicable to the user’s role) | SHOULD | NHSBT | 1. Each user has access to the functionality they are entitled to based on their user profile | Head of Information Security |  |
| Passwords MUST implement a minimum standard of complexity as defined by NHSBT. | MUST | NHSBT | 1. System requests user for a password that meets required complexity | Head of Information Security |  |
| The solution must allow system owners to review access permissions regularly. | MUST | NHSBT | 1. System owner once logged in can review access permissions | Head of Information Security |  |
| The solution must allow users that leave the organisation to be removed from the system in line with NHSBT Policy | MUST | NHSBT | 1. It must be possible to remove a user from accessing the system once removed from active users list | Head of Information Security |  |
| The solution should ensure that active sessions for a user are limited to one per user. | SHOULD | NHSBT | 1. User cannot open more than on active session | Head of Information Security |  |
| The solution must ensure that every user has a unique ID/system login attributable only to them. | MUST | NHSBT | 1. It is not possible to have more than one unique id per user | Head of Information Security |  |
| 2. Any unique id must not be attributable to more than one user |  |
| The solution must ensure that user accounts logged on to the system must time-out after a pre-defined period of inactivity. | MUST | NHSBT | 1. User is logged in | Head of Information Security |  |
| 2. x amount of inactivity |  |
| 3. System must time out and request user to log in again |  |
| The solution must comply with POL 10 | MUST | NHSBT |  | Head of Information Security |  |
| All user access to the system must be compliant with the NHSBT Security Policy | MUST | NHSBT | An approved access provisioning process. | Head of Information Security |  |
|  |
| The solution must have the ability to continuously integrate patches and fixes. | MUST | Supplier | Supplier approved process | Head of Service Management |  |
| Services must achieve WCAG 2.1 level AA as part of meeting government accessibility requirements. | MUST | NHSBT | Accessibility Compliance Testing | TBC |  |
| Browser apps should not require plugins. | SHOULD | Supplier | Supplier Technical Specification | TBC |  |
| Systems that use a browser should be designed responsively, such that screens are rendered well regardless of browser or device | MUST | Supplier | Supplier Technical Specification | TBC |  |
| User authentication of the solution should support federated authentication and follow the SAML (Single Sign-on) standard. | SHOULD | Supplier | Approved, auditable Process | Head of Information Security |  |
| The solution must ensure that email communications are sent from a recognisable corporate email address | MUST | NHSBT | Approved/auditable joiners process | Head of Information Security |  |

# Appendix C – Document Reference

## DOCUMENT LOCATION

Hard and soft copies of this document are uncontrolled and may not therefore be current. The approved source of this document can be found at:

* NHSBT– Transitions/Transformation <<Link to File Share>>
* With the author (if in an unapproved status)
* Enter location of issued document for if stored on local <<project>> repository

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Signatories** | | | |
| Reviewer(s) | Name / Role  Description | | Date |
| Craig | Solutions Architecture and Data Management | |  |
| Lisa Burnapp | Subject Matter Expert | |  |
| Joel McGrath | Product Owner | |  |
| Matt Thorogood | Business Analyst | |  |
|  |  | |  |
| Approvers(s) | Name / Role | Signature(s) | Date |
|  | Business/Product Owner |  |  |
|  | Quality Lead |  |  |
|  | Business Analysis |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Amendment Record** | | | | |
| Issue No. | Amendment Detail | Author | Date | Approved |
| 0.1 | Initial draft | Matt Thorogood | 04/12/2020 |  |
|  |  |  |  |  |