STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Change Control**
Effective Date:	**22 Jul 2019**
Reference Number:	**SOP-03-08**
Version Number:	**3.0**
Owner:	**Information Security Manager,**
Review Date:	**22 Jul 2021**

Table of Contents

1. Purpose

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

This document defines the process for managing changes to the Trustworthy Research Environment.

2. Scope

The TRE system, including all supporting infrastructure within the data room at Vaughan House. This includes all server, network, power and cooling hardware. It also includes all software installed to operate the infrastructure, and to support the transfer of data into the TRE.

Only 3rd party software is installed in TRE system, therefore software development is not within the scope of this procedure.

3. Responsibilities

The TRE Infrastructure and Security Management Process Owner is responsible for:

- Approving change requests

The TRE Operations Manager is responsible for:

- Approving change requests when deputising TRE Infrastructure and Security Management Process

The TRE Operations Team are responsible for:

- Receiving and processing request for change
- Ensuring all change request correspondence is adequately recorded

The TRE System Administrator is responsible for:

- Only acting upon changes specified in the TRE Infrastructure Record (exceptions are made for emergency situations)
- Ensuring all changes to the TRE are adequately recorded in the TRE Infrastructure Record

4. Procedure

Changes made to the TRE infrastructure must be controlled and conducted in a consistent manner. This helps lower the risks associated with making changes.

4.1. Change Control workflow

The standard Change workflow comprises the following:

- Receive request
- Create a record of the request
- Triage the request
- Conduct risk assessment for the request
- Devise 'backout plan' if necessary
- Raise a Request for Change (RFC) if necessary
- Approve the change

- Implement the change
- Post-implementation review

4.2. Source of Change

A change may involve any of the following:

- The initial setup of a new TRE Project virtual working environment
- System upgrade (e.g. routine software updates/patches)
- System development (modification)
- Bug fixes (software)
- Relocation of assets
- Adding or removing software or hardware components
- Planned/Unplanned hardware maintenance
- Replacing assets following failure or end-of-life
- Altering configurations (server and/or network devices)

There are two sources of change request:

1. Internal: Changes to infrastructure as a result of planned and unplanned development, upgrades, maintenance, patching, renewal and replacement.
2. External: Changes to the specification and/or magnitude of computational and data storage resources provided to TRE users, usually in response to formal requests made to live projects, or when first setting up a TRE project.

All of the above changes may introduce new issues that could impact on the ability of the TRE to provide reliable and secure services. This could be caused by a vulnerability inherent within the new or modified component or control. This can be termed a 'post-implementation' risk.

There is also the risk that an issue may occur during, and as a direct result of the work being carried out to implement the change. These can be termed an 'implementation' risk.

Some changes are very risky to implement, but once completed, they provide benefits that outweigh the implementation risks. Conversely, some changes are quite easy to implement, but they could introduce new risks, and therefore it is essential to avoid the temptation to make such changes without first anticipating any new threats that will arise. Formal risk assessment is the methodology for anticipating threats.

4.3. Change Risk Assessment

The first stage of risk assessment is to identify the threats to the Confidentiality, Integrity and Availability (CIA) of TRE data that could occur during and after the change is conducted. In accordance with ISMS-02-05 Risk Management Process, it is necessary to determine the impact of these threats, and also the likelihood of them occurring, representing them as numerical values to calculate an overall risk factor, or score:

Risk Impact = Maximum of Confidentiality, Integrity or Availability

Risk Score = Risk Impact x Likelihood

Example:

Confidentiality	= 3
Integrity	= 2
Availability	= 5
Likelihood	= 4

Risk Score = 5 x 4 = 20

Table 1: Risk Level and Approval

Score Range	Risk level	Change Type	Risk Assessment	Approval Action	Method of recording work activity
1-5	Low	BAU	Pre-determined with a level of 'Low'	RFC not required, automatic approval	N/A
1-5	Low	Standard	Pre-determined with a level of 'Low'	RFC not required, approval by ISM	TRE Infrastructure Record
6-12	Low	Normal	Risk assessment required	RFC not required, approval by ISM	TRE Infrastructure Record
6-12	Medium	Normal	Risk assessment required	RFC required approval by TRE Project Board	TRE Infrastructure Record and RFC
13-25	High and Very High	Normal	Risk assessment required	RFC required approval by ISSG	TRE Infrastructure Record and RFC

Details of the risk assessment are recorded within the applicable worksheet of the TRE Infrastructure Record. A copy of the risk description is copied into the RFC form.

When calculating the risks associated with carrying out the work to implement the change, it is important to consider whether it is possible to revert back to the last known working state. This is often termed the 'backout plan'. If a backout plan exists, the likelihood associated with a particular risk can usually be given a lower score.

If the change has been successfully carried out on previous occasions, this can also determine the likelihood associated with the overall risk of conducting a change. The consequence of having made a change before also allows a change 'type' to be determined.

4.4. Change Type

Some changes are conducted routinely, and can be described as 'Business as Usual (BAU).

As shown in Table 1, BAU changes do not require approval, and there is no formal request record within the TRE Infrastructure Record. BAU changes have a pre-determined risk level of 'Low'.

A 'Standard' change also has a pre-determined risk level of 'Low' but requires approval by the ISM, and the request details must be recorded in the TRE Infrastructure Record.

All other changes are considered to be 'Normal', which means there is some uncertainty about the likelihood of a successful implementation, and therefore risk assessment must be conducted. If the resulting risk level is 'Low', the ISM can approve the change. If the risk level is above 'Low', approval requires more input, as defined in Table 1.

Apart from BAU, all changes must be described within the TRE Infrastructure Record using the worksheet corresponding with the nature of the change request.

4.5. Change Review, Assessment, Approval and Action

The triage stage of change control is conducted by the ISM, and if the ISM is not available, this task can be delegated to a CHI Information Systems Programme manager. The triage stage determines if the proposed change comes from a valid source (section 4.2 can be used as a guideline).

The ISM or a CHI Information Systems Programme manager then conducts the risk assessment, which determines whether an RFC must be completed and who must approve the RFC.

Table 1 defines which person or group is responsible for approval. The TRE Project Board meeting in person every 2 weeks, but approval can be sought via email for more urgent matters. At least one member of the CHI Senior Management Team (SMT) must participate in the approval process when the TRE Project Board are conducting the RFC review.

The ISSG only meet every 2 months, so in most cases, approval for RFCs will most likely be conducted via email, and not face to face meetings. ISSG review and approval can be conducted if there are no more than 2 members unable to participate.

The TRE Operations team meet each week to review and either approve or reject formal change requests, or to agree change such as planned maintenance, or to discuss, review and schedule unplanned maintenance or incidents. Time critical issues are discussed via email in between meetings.

The TRE System Administrator may only respond to requests to carry out change to the TRE that have been communicated to the tre-admin@manchester.ac.uk mail box, and have been sent by either the ISM or a CHI Information Systems Programme manager. This is an internal mail box. Messages sent to this address provide the context of the required change and reference the applicable section of the TRE Infrastructure Record that contains the full details of the change. For Standard changes, all the required information is stored in the applicable worksheet and the RFC field will be marked 'N/A'. For Normal changes, the required information is stored within the 'Project Tasks' or 'Core Infrastructure' worksheets within the TRE Infrastructure Record, and further details are specified within the RFC form.

Only the ISM or a CHI Information Systems Programme manager can modify the TRE Infrastructure Record. Any member of TRE Staff can fill in an RFC, but only the ISM or a CHI Information Systems Programme manager can submit an RFC for approval.

The exception is if an emergency change must be immediately carried out to prevent serious risk to TRE data and end-users, but it is still necessary to update the Infrastructure Record retrospectively after the event.

4.6. Emergency Change

In the event of an emergency situation and where both the ISM and a CHI Information Systems Programme manager are unavailable to approve the change, the ISMS Sponsor has the authority to provide approval.

4.7. Change Notification

TRE stakeholders only require immediate notification of change if it is unplanned. In such cases, for example an unplanned service outage, a best efforts approach is carried out to inform TRE users and other affected individuals via email messages sent manually by the TRE Operations team via the tre-support@manchester.ac.uk mail box.

TRE users who have made a request to the TRE Operations team will be kept informed of progress.

4.8. Change Record-Keeping

There are three separate information systems used to record all information related to TRE change, all of which require user account authentication for access:

- *JIRA – TRE projects*
- *Q-Pulse*

TRE users complete FORM-002 for the initial project request and FORM-007 for user-requested changes to existing TRE projects, including requests for data exports. Each TRE project is managed by a record within JIRA (Link to JIRA). Copies of completed forms are attached to the corresponding project records.

RFCs are recorded using FORM-008. These documents must only be made visible to TRE Staff, the TRE Project Board and the ISSG. RFC forms are stored in Q-Pulse as an attached object to the TRE asset most impacted by the change. In the event of a change that affects multiple assets, a best effort must be made to establish the primary 'parent' asset, whose Q-Pulse asset record will contain the RFC.

Q-Pulse hosts numerous asset registers, each covering a particular aspect of the TRE infrastructure and TRE datasets. If a change to a component of the TRE infrastructure takes place, for example replacement of a fault CPU fan, a record of that change will be recorded in the corresponding asset record using the built in 'Non-Conformance' generator.

- *TRE Infrastructure Record*

The TRE Infrastructure Record is an Excel spreadsheet stored within the Centre for Health Informatics' eLab system. The location on the eLab* server is:

Site: Trustworthy Research Environment
Folder: Records
File: TRE Infrastructure Record.xlsx

The details of the request for change approved by the TRE Operations team must be typed into the TRE Infrastructure Record, such that the instructions for performing that change are made clear to the person carrying out those tasks. Depending the scale or complexity of the requested change added to the TRE Infrastructure Record, it may be necessary to create a JIRA record to provide supplementary information. Document SOP-03-20 describes this process in more detail.

* The eLab server is a Centre for Health Informatics built and hosted secure repository of operational and research information. Access to the eLab server's Trustworthy Research Environment site is only granted to members of the TRE Operations team.

- *Request for Change (RFC) form*

Document FORM-008 must be completed for each Request for Change. The form comprises three sections:

- Details of change request and risk assessment
- Change review and approval
- Change closure checklist

4.9. Performing Changes to the TRE

The TRE Infrastructure Record.xlsx acts as an intermediary between the approved requests for change, and the act of physically performing those changes to the TRE infrastructure. The TRE system administrator or any other member of the TRE Operations team authorised to perform changes to the TRE are only permitted to follow requests specified via the TRE Infrastructure Record. Changes to TRE infrastructure that have not been specified within the TRE Infrastructure Record are not authorised to be completed. The exception to this rule is emergency changes, which are described within the TRE Business Continuity Plan.

The procedure for filling in the change request details are contained within the first worksheet of the TRE Infrastructure Record.xlsx file. This procedure can be summarised by stating that each field within the spreadsheet has a unique alphanumeric location defined by the parent column header and row number. The uniqueness of these locations ensures that a request to perform the change defined within a given field is clear and unambiguous, which means the likelihood of a TRE system administrator carrying out the wrong change is acceptably low. As each entry into the TRE Infrastructure Record must be timestamped, it also ensures that a historical and auditable account of all TRE change exists.

The TRE System Administrator will fill out the applicable fields within the TRE Infrastructure Record to reflect the actual changes made to the TRE, including any specific technical details such as hardware and software identifiers.

5. Cross-referenced ISMS Documents

Number	Type	Title
FORM-008	ISMS\Forms	TRE Request for Change
FORM-002	ISMS\Forms	TRE Project Application Form
FORM-007	ISMS\Forms	TRE Project Service Request Form
ISMS-02-05	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Risk Management Process
SOP-09-17	ISMS\SOP\TRE System Administration - SOP	Testing Continuity of TRE Security
FORM-008	ISMS\Forms	TRE Request for Change
SOP-05-01	ISMS\SOP\Asset and Supplier Management - SOP	Bringing Assets into the TRE
SOP-03-24	ISMS\SOP\TRE Operations - SOP	Migrating Projects out of the TRE
ISMS-03-03	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Disaster and Severe Incident Recovery Plan
SOP-03-09	ISMS\SOP\TRE Operations - SOP	TRE Project Application Review
SOP-03-20	ISMS\SOP\TRE Operations - SOP	Managing Security Development Tasks
SOP-09-18	ISMS\SOP\TRE System Administration - SOP	Testing Segregation of TRE Projects

6. Appendices

None