POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Disaster and Severe Incident Recovery Plan**
Effective Date:	**13 Nov 2019**
Reference Number:	**ISMS-03-03**
Version Number:	**2.0**
Owner:	**Information Security Manager,**
Review Date:	**13 Nov 2021**

Table of Contents

1. Purpose

The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. The organization should also establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

This document defines the procedure for declaring a disaster affecting the Trustworthy Research Environment (TRE) and provides guidance for the emergency steps to manage the TRE during a disaster or other adverse situation and any period of system recovery to maintain Business Continuity and Information Security.

The term “adverse situation” is any situation that significantly impacts:

- The availability of the TRE service, Vaughan House, personnel and assets
- The confidentiality of information in the TRE
- The integrity of the information and assets under the scope of the TRE.

2. Scope

This procedure includes for managing the disaster recovery planning for the TRE. The disaster recovery plan will only include for the recovery of the critical systems and essential communications.

The recovery of the University of Manchester infrastructure and services on which the TRE is dependent are excluded from the scope.

Recovery from any adverse situation that will require a full bare metal rebuild is out of the scope of this procedure since CHI will be unable to complete this activity.

3. Responsibilities

3.1. Contacts for Declaring a Disaster

The following individuals are the primary contacts for declaring a disaster and activating the disaster recovery plan.

Name	Job role	Contact details	DR Responsibility
	ISMS Management Sponsor, ISSG Board		Declaring a disaster
	ISSG Board		Declaring a disaster (1st deputy)
	ISMS Management Process Owner, ISSG Board		Declaring a disaster (2nd deputy)
	ISMS Communications Process Owner		Communication disaster to impacted stakeholders
	ISM,		Communicating to

	ISSG Board		impacted stakeholders (1st deputy)
	TRE Infrastructure and Security Management process owner, ISSG Board		Communicating to impacted stakeholders (2nd deputy)

3.2. Contacts For Restoring Services

The following individuals are to assume responsibility for restoring the critical TRE services when the DR plan is activated:

Name	Job role	Contact details	DR Responsibility
	TRE System Administrator		Restoring TRE service
	TRE Infrastructure and Security Management process owner		Developing recovery plan and providing resources to restore TRE service
	ISM, ISSG Board		Managing RFCs throughout system recovery

4. Procedure

4.1. Identifying and Declaring a Disaster

A "disaster" is any adverse situation that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operation of the TRE.

This can include:
- Loss of power
- Loss of network
- System security/data breach
- Fire
- Flooding
- Other natural disaster
- Events affecting key staff availability

Resulting in:
- Damage to or loss of infrastructure
- Loss of building or building access
- Loss of key services (e.g. power or network)
- Loss of data
- Reduction in staff

The person discovering the incident must notify the primary contact(s) for declaring a disaster. The primary contact will have responsibility for deciding if the disaster recovery plan should be

implemented and the disaster communicated to TRE users, relevant authorities, CHI management and employees. The primary contact should also decide who should be involved in the disaster recovery process (e.g. ISSG members and process owners).
When a serious incident occurs the primary contact should also consider any potential legal and reputational risks that go beyond the scope of the TRE itself and ensure these are also addressed as part of the disaster management process e.g. a data breach may present UoM level legal and reputational risks

The disaster recovery plan is to be activated when one or more of the following criteria are met:
- Service forecast to be unavailable for > 20 days
- Reduced service available for > 1 month

4.2. Disaster Recovery Plan

4.2.1. Communicating to Stakeholders

In the event of communicating a planned or unplanned outage to the service an email will be sent to all stakeholders by the Communication process owner. This will be completed within 24 hours of the disaster being declared.

The stakeholders will include:
- All TRE staff
- All TRE users
- Key sponsors
- CHI staff and students

Disaster notifications should include the following:
- Reason for message
- Part of service affected
- Expected date service will resume

Further communication will be sent as appropriate to inform users of any changes to the forecast recovery schedule.

4.2.2. Initial Actions

If the service is still operational (to any degree) it shall be shut down in a controlled manner. For a suspected data breach it is permissible to immediately disconnect the WAN network cable from the external interface of the perimeter firewall.

4.2.3. Recovery Process

Depending upon the exact nature of the disaster the recovery process may include some or all of the following activities.
- Relocation of existing hardware to an approved UoM data centre
- Renewal or repair of hardware in existing location
- Restoring data from backup
- Training new personnel

The TRE infrastructure is not duplicated in an alternative datacentre so there is no separate environment to allow for recovery of the system.

A documented recovery plan should also be created at this point by the TRE Infrastructure and Security Management process owner to make it clear what actions are needed, who is responsible and the timelines for recovery.

The recovery plan may utilize the TRE data backup and restore procedure (ISMS-09-11).

4.2.4. Service Level for System Recovery

The TRE Service is managed by the TRE Operations Team. Normal working hours are between 09:00 and 17:00 Monday to Friday.

The TRE Operations team do not offer a service level agreement for users of the TRE service that defines the response times for adverse situations. There is no guarantee made for the availability of the TRE service, whether stated as a percentage of 'up-time' or an absolute amount of time that will elapse before the service is resumed. The forecast schedule for restoration of the service will be communicated as part of the initial disaster communication to stakeholders. Further updates will be distributed as the schedule is more clearly established during the recovery period.

4.2.5. Business Continuity

If the TRE becomes unavailable due to an adverse event there is no provision by CHI for business continuity (i.e. continued access to TRE data or provision of TRE services) during the period of unavailability. Managing the continuity of any activity related to the TRE data (e.g. research) is the responsibility of the TRE users, although it is recognized that no activity may be possible without the TRE.

4.2.6. Critical Systems for Recovery

The critical systems that shall be restored are as follows:

- Perimeter firewall
- Network switches
- Infrastructure supporting servers
- Storage controllers
- Services
- TRE Projects
    - Active projects

TRE Change Control (SOP-03-08) will be used to manage the necessary steps to restore and restart the service through a series of Request for Change (RFC). This process will include the testing of the individual components of the service

4.2.7. Security Test of Restored Service

The security of the restored service will be tested prior to go-live in accordance with SOP-09-17 Testing

Continuity of TRE Security.

4.2.8. Approval to Go-live with Restored Service

The restoration of services will depend upon the nature of the disaster and the approval criteria should be included in the disaster recovery plan e.g. after a suspected security breach this would be after an appropriate investigation has been completed and approval may need to be given by central UoM Information Governance / Information Security; for a power or network loss the system could be restored once the services are returned.

The ISSG will approve each RFC related to the restoration of individual services or components within the TRE (these changes are considered to be outside of the approval scope of the normal change control process). The ISMS Management Sponsor (or deputy) will approve the work to reconnect the perimeter firewall back to the external facing network, e.g. the University or HSCN networks.

4.2.9. Communication of Go-live to Stakeholders

Following approval to go-live an email will be sent to all stakeholders by the Communications process owner informing them when the service will be restored.

4.3. Disaster Recovery Plan Testing Schedule

The DR plan will be tested in its entirety on a yearly basis.

4.3.1. Test Scenarios

A test scenario should address the recovery process for one of the following potential adverse events.

Event ID	Adverse Event	Might lead to….	Description of threat to TRE Infrastructure and/or Data	Recovery process	Test Simulation	Recovery Process to Test
1	Fire in Server Room	Damage to infrastructure	Loss of availability, disruption to service. Permanent destruction of all local storage devices and therefore loss of all data stored locally	Renewal or repair of some hardware. Data restore. Relocation of physical server room.	n/a	Restore data from backup
2	Fire (not in Server Room)	Damage to infrastructure, power cut	Dependant on location of fire at VH. Close proximity could result in heat or smoke damage to the TRE infrastructure, or perhaps a power-cut	Renewal or repair of some hardware. Data restore	n/a	Restore data from backup
3	Electrical Outage	Power Cut	The TRE infrastructure is powered through a UPS device which can keep everything running for about 20 minutes in the event of a power cut. Once the UPS batteries have run out, all electrical power to the TRE will be cut, resulting in all servers and storage devices immediately halting.	Managed start-up of service	Trip master power switch in server room or forced immediate shutdown on hypervisors	System start-up routine
4	TRE Hard Disk Failure	Loss of data, disruption to data and config backup	Availability and possibly integrity although both cases are unlikely, as all storage volumes are support by a multi-disk RAID configuration which means loss of a single disk should have no immediate effect. But in the event the RAID array become compromised, this can lead to corruption of data.	Renewal or repair of associated hardware. Data restore	Pull disk or other component out of machine while running	Restore data from backup
5	TRE Storage Array Failure	Loss of data, disruption to data and config backup	Availability and integrity of data can be compromised	Renewal or repair of associated hardware. Data restore	Pull disk or other component out of machine while running	Restore data from backup

Event ID	Adverse Event	Might lead to….	Description of threat to TRE Infrastructure and/or Data	Recovery process	Test Simulation	Recovery Process to Test
6	TRE Perimeter Firewall Failure	Loss of network traffic, or loss of perimeter security	Availability of data if network connection is lost, or confidentiality of data if firewall filtering becomes disabled	Renewal or repair of associated hardware. Data restore	Power off perimeter firewall	Restore data from backup
7	Network Failure	Loss of service	Availability of data in the event of a long outage period.	Directing users at alternative service, e.g. using a fail-over mechanism	Power off the perimeter firewall, or disabling a master inbound traffic rule.	Not necessary (availability only)
8	DDoS Attack	Disruption to service and possibly reputation	Loss of availability, disruption to service	Directing users at alternative service, e.g. using a fail-over mechanism	n/a	Not allowed
9	Members of staff are unable to come to work due to events including: - Public transport strike - Severe weather - Fuel shortage - Public disorder	Reduction in Staff	Lack of personnel could mean it takes longer to recover a service in the event if failure, and an increased likelihood of an event because there are less people monitoring the overall service. The main impact would be the availability	Training new personnel	We could ensure sys-admin procedures are written in a manner that almost any member of staff could conduct critical tasks such as service or data recovery	Not feasible to test
10	Members of staff are unable to work from any location due to events including: - Flu pandemic	Reduction in Staff	Lack of personnel could mean it takes longer to recover a service in the event if failure, and an increased likelihood of an event because there are less people monitoring the overall service. The main impact would be the availability	Training new personnel	We could ensure sys-admin procedures are written in a manner that almost any member of staff could conduct critical tasks such as service or data recovery	Not feasible to test
11	Natural disaster including: - Earthquake - Meteor strike	Damage to infrastructure	Loss of availability, disruption to service. Permanent destruction of all local storage devices and therefore loss of all data stored locally	Renewal or repair of some hardware. Data restore	n/a	Restore data from backup

Event ID	Adverse Event	Might lead to….	Description of threat to TRE Infrastructure and/or Data	Recovery process	Test Simulation	Recovery Process to Test
12	Severe flood caused by weather or building water supply	Damage to infrastructure	Availability and possibly integrity could be compromised. As server room is on ground floor, any water seeping into this area will possibly lead to an electrical power cut as the UPS is on the floor, and the bottom rack spaces are hosting servers.	Renewal or repair of hardware. Data restore	n/a	Restore data from backup
13	Theft or vandalism	Damage to infrastructure	Loss of availability, disruption to service. It is not expected that stolen infrastructure could be used to access TRE data	Renewal or repair of hardware. Data restore	n/a	Restore data from backup

4.4. Adverse Situation Information Security Continuity

In the event of an adverse situation the ISMS information security controls and classifications still apply and must be followed. No action to maintain the availability of the TRE service at the expense of continuity of information security will be allowed. A number of features allow information security to be maintained in the existing server room in the event of an adverse situation:

- The entrance door to the server has a physical key-lock in addition to the electronic swipe-card lock. This ensures the door remains locked during electrical failure and when the Vaughan House fire-alarm is activated
- All critical TRE data objects replicated on a daily basis to an internal storage device. Restoring these backups is tested routinely in accordance with ISMS-09-17 Testing Continuity of TRE Security
- All data is encrypted to AES256 while stored and transferred internally. It is only decrypted while being processed in memory with the encryption key only residing in memory at the point the virtual machine has booted. This means the data on a storage drive is always in an encrypted state, and in the event of a power cut, or if a disk is removed at any time, the data will not be accessible
- Due to the lack of labelling on devices, it would be highly improbable that theft of one or more machines from the server room would allow the perpetrator to re-build the Cloud array in a way that data could be accessed
- The server room UPS ensures power is continually supplied to TRE compute infrastructure. This helps prevent any damage, loss or compromise to the integrity of data in the TRE in the event of a power cut to the server room
- University Estates Security monitor the local area on foot and via CCTV which means in the event no CHI or TRE staff are present, a reasonable level of monitoring takes place

5. Cross-referenced ISMS Documents

Number	Type	Title
SOP-09-17	ISMS\SOP\TRE System Administration - SOP	Testing Continuity of TRE Security
SOP-03-08	ISMS\SOP\TRE Operations - SOP	TRE Change Control
ISMS-03-08	ISMS\Policy & Guidance\TRE Operations - policy & guidance	TRE Maintenance Policy
ISMS-09-07	ISMS\Policy & Guidance\TRE System Administration - policy & guidance	TRE Key Management Policy

6. Appendices

None