

# ICT Service Disaster Recovery Plan for Serco Contract

Serco UK & Europe at Thurrock Council

## ICT 3rd Floor Civic Offices II

A copy of this Plan is to be retained by  
all the ICT services team managers

<b>Author</b>	<b>Andy Best</b>
<b>Version</b>	<b>3.1</b>
<b>Sign off by</b>	<b>Steve Abbott</b>
<b>Date of sign off</b>	<b>22/01/15</b>

*'This plan has been reviewed by Phoenix in Conjunction with Serco  
and is based on the Thurrock Council standard template'*

**Appendices attached to this plan that contain personal information must be kept confidential to comply with the relevant provisions of the Data Protection Act 1998 or any subsequent Legislation that enacts similar provisions.**

## Document Control

Version History			
Version	Date	Reason for release	Issued by
2.1	02/01/14	Review to cover new services	A Best
3.0	02/12/14	Annual Review	A Best

Document Approval		
Role	Name	Date approved
Head of ICT	Steve Abbott	02/12/13

Document Distribution		
Role	Name	Organisation
Service Delivery Manager	Andy Best	ICT
Applications Manager	Gerry Waterfield	ICT
Business Services Manager	Clive Denham	ICT
Joe Gregory	SandI Team Leader	ICT
Gary Malley	CandI Team Leader	ICT
Aaron Page	Servicedesk Team Leader	ICT

Document Reference	
Document	Location
IT Service Disaster Recovery Plan	J:\ICT\08 BAU\Business Continuity

Last Review Date	
Review Date	Reviewer
14/11/2014	A Best

# Table of Contents

Table of Contents .....	3
Plan Revision History .....	5
About This Disaster Recovery Plan .....	6
1.1. Purpose and Scope of This Plan .....	6
1.2. Updating This Plan .....	6
1.3. Distribution List .....	6
2. Plan Objectives .....	8
3. Recovery Teams and Responsibilities .....	9
3.1. ICT Disaster Management Team (DMT) .....	9
3.2. Service Delivery Team .....	10
3.3. Application Support SandI Team .....	11
3.4. Council / Facilities (Non-ICT) .....	12
4. What to Do in the Event of a Disaster .....	13
4.1. Standard Emergency Procedures .....	13
4.2. The First Steps for the Recovery Teams .....	13
4.3. The Next Steps .....	13
5. Recovery Scenarios .....	14
5.1. Civic Offices (data centre or building) .....	14
5.2. Derby Road Bridge .....	14
5.3. Tasmania House .....	14
5.4. ICT Resources .....	15
6. Recovery Activities .....	16
6.1. ICT Disaster Management Team Tasks .....	16
6.2. Service Delivery Team Tasks .....	17
6.3. Application Support SandI Team Tasks .....	18
6.4. Application Support CandI Team Tasks .....	19
6.5. Facilities Team Tasks (ICT related) .....	20
7. The Command Centre .....	21
7.1. Primary Command Centre .....	21
7.2. Alternative Command Centre .....	21
7.3. Command Centre Requirements .....	21
8. The Standby Facility .....	22
8.1. Location of the Standby Facility .....	22
8.2. Standby Alert Confirmation Sheet (only for a 3 <sup>rd</sup> party agreement) .....	22
8.3. Standby Data Centre requirements .....	23
9. The Data Storage Location(s) .....	24
9.1. Backup Media .....	24
9.2. DSL (definitive software library) .....	24
10. Critical Business Services .....	25
Critical Services – Phase 1 & 2 .....	25
11. Directories .....	27
11.1. Recovery Team Members .....	27
11.2. User Groups and Application Support .....	29
11.3. Vendor and Supplier Contacts .....	31
12. Inventories .....	33
12.1. Computer Hardware .....	33
13. Recovery Critical Path Plan .....	34

14. Service Recovery Procedure list .....	35
Appendix A .....	37

# Plan Revision History

It is important that this ICT Service Disaster Recovery Plan accurately reflects the current situation and business requirements at Thurrock Council. Updates must be provided to the DR process owner.

The following table describes the history of this document.

<b>Version</b>	<b>Date Issued</b>	<b>Reason for Update</b>
1.1		Initial Draft
1.3		Name and role changes
1.4	26/08/2011	Review following restructure of ICT department
1.5	03/08/2012	Review following department restructure and recent staff changes.
1.6	09/10/2013	Updates following department re-structure
1.7	14/11/2013	New format for front pages
2.0	02/01/2014	Annual review
2.1	14/11/2014	Review following new services being introduced
3.0	05/122014	Annual Review

This plan is reviewed annually or upon changes to staff/structure.

The next review is due 14 November 2015.

# About This Disaster Recovery Plan

## 1.1. Purpose and Scope of This Plan

This plan has been designed and written to be used in the event of a disaster affecting Thurrock Council at Civic Offices, New Road, Grays, Essex, RM17 6SL.

This plan is structured around teams, with each team having a set of specific responsibilities.

The decision to initiate disaster recovery procedures will be taken by Thurrock Council's Disaster Management Team Leader or their deputy after assessing the situation following a disaster or crisis.

If the Council's Disaster Management Team invokes the disaster recovery procedures, then all members of the ICT Disaster Recovery Team will follow the procedures contained in this plan until recovery is complete.

This plan contains all the information necessary for Serco to restore an operational ICT service, for the elements they are responsible for as defined in the strategic services partnership, in the event of a serious disruption of computer services at Civic Offices.

## 1.2. Updating This Plan

This plan must be kept up to date.

It is the responsibility of the ICT Service Delivery manager to ensure that procedures are in place to keep this plan up to date. If, whilst using the plan, you find any information which is incorrect, missing or if you have a problem in understanding any part of this plan please inform the ICT Service Delivery manager so that it may be corrected. It is important that everyone understands their role as described in this plan.

Updated versions of the plan are distributed to the authorised recipients, listed in Section 1.3, Distribution List.

## 1.3. Distribution List

The ICT Service Delivery Manager is responsible for the distribution of this plan. Each plan holder, listed in the table below, receives a copy of this plan. The plan, and associated documents, will be replicated to the laptops of the ICT Disaster Recovery Team, with a further copy stored offsite on the Culver Centre DC server.

The Service Delivery Manager will periodically check that the software distribution of the plan is occurring

Name	Name	Deputy
------	------	--------

Account Partnership Director	Ian Cousins	Jacqui Harding
ICT Head of Service	Steve Abbott	Clive Denham
Service Delivery Manager	Andy Best	Gerry Waterfield
Support Services Manager	Gerry Waterfield	Andy Best
CandI Team leader	Gary Malley	Gerry Waterfield
SandI Team Leader	Joe Gregory	Gerry Waterfield
Offsite Copy 1	Serco Our World Portal	
Offsite Copy 2	DR team Laptops	

## 2. Plan Objectives

A disaster is defined as an incident which results in the loss of computer services at the Thurrock Council sites at Civic Offices or Tasmania House, to the extent that relocation to a Standby Facility is required. A disaster can result from a number of accidental, malicious or environmental events such as fire, flood, terrorist attack, human error and software or hardware failures.

The primary objective of this ICT Service Disaster Recovery Plan is to ensure the continued operation of identified business critical systems in the event of a disaster.

Specific goals of the plan are:

- To restore services in priority order and for high priority services to be operational at a standby facility made available by Thurrock Council within 3 working days of it being available and subject to replacement equipment being sourced from suppliers.
- To operate at the standby facility for as long as required
- To reinstate Thurrock Council ICT services in the Thurrock Council Civic Offices premises or an alternative designated facility To minimize the disruption to Thurrock Council's business



# 3.Recovery Teams and Responsibilities

This section defines the functional responsibilities of the ICT Recovery Team.

## 3.1. ICT Disaster Management Team (DMT)

The ICT Disaster Management Team is responsible for providing overall direction of the data centre recovery operations. It ascertains the extent of the damage, activates the ICT Disaster Recovery Team, and notifies the team members. Its prime role is to monitor and direct the recovery effort.

The Council Disaster Management Team is responsible for deciding whether or not the situation warrants the introduction of disaster recovery procedures. If they decide that it does, then the ICT Disaster Management Team defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The ICT DMT should nominate a DR Team Leader. The DMT operates from the Command Centre or via conference calls.

### 3.1.1. ICT Disaster Management Team Responsibilities

The ICT Disaster Management Team is responsible for the following:

- Making decisions about restoring the computer processing environment in order to provide the identified level of operational service to users.
- Managing all the ICT recovery teams and liaising with Thurrock Council's management, Serco public sector regional management, Serco Global Technology Division (GTD), blue light services and users, as appropriate.
- Maintaining audit and security control during the recovery from disaster.
- Identifying, controlling and recording emergency costs and expenditure.
- Evaluating the extent of the problem and potential ICT consequences.
- Notifying Council Stakeholders of the recovery progress and problems.
- Initiating ICT disaster recovery procedures.
- Liaising with 3<sup>rd</sup> party suppliers to co-ordinate service restoration
- Coordinating recovery operations.
- Monitoring recovery operations and ensuring that the schedule is met.
- Documenting recovery operations.
- Liaising with business management.
- Monitoring computer security standards.
- Ensuring that appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing.
- Ensuring change management processes are followed
- Provide updates to the wider Serco service Disaster recovery operations
- Declaring that the ICT Service Disaster Recovery Plan is no longer in effect when computer processing is restored at the primary site.
- Provide ICT staff with information on where they need to report to.

## 3.2. Service Delivery Team

The Service Delivery Team is responsible for the computer environment (not the “fabric” - which includes the building, power provision, HVAC, security, fire detection/suppression, etc in the computer room and other Comms rooms) and for performing tasks within those environments. The Service Delivery Team consists of members of the SandI , CandI , 3<sup>rd</sup> party suppliers, Service desk and 2<sup>nd</sup> Line support teams.

This team is responsible for restoring the Council’s ICT services and for performing the activities required to achieve this.

### 3.2.1. Service Delivery Team Responsibilities

The Service Delivery Team is responsible for the following:

- Ensuring that the standby equipment meets the recovery schedules.
- Installing the computer hardware and operating systems at the standby facility.
- Setup of a standby Service Desk facility
- Obtaining all appropriate historical/current data from the offsite storage location and restoring up to date:
  - Infrastructure services
  - Application systems
  - Shared data volumes
- Providing the appropriate management and staffing of the standby Data Centre and Service Desk to meet the defined level of business requirements.
- Performing backup/recovery activities at the standby site.
- Providing ongoing technical support at the standby facility.
- Working with the SandI Team to restore local and wide area data communications services to meet the minimum processing requirements.
- Initiating operations at the standby facility.
- Re-establishing the Service Desk and Media Control/Tape Library functions at the standby facilities.
- Establishing interim processing schedules and inform user contacts
- Arranging for acquisition and/or availability of necessary computer supplies
  
- Ensuring that all documentation for standards, operations, vital records maintenance, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate.
- Arranging new local and wide area data communications facilities and a communications network, which links the standby facility to the critical users
- Installing a voice network to enable identified critical telephone users to link to the public network.
- Evaluate the extent of damage to the voice and data network and discuss alternate communications arrangements with telecoms service providers.
- Establish the network at the standby facilities in order to bring up the required operations.
- Define the priorities for restoring the network in the user areas.
- Order the voice/data communications and equipment as required.

- Supervise the line and equipment installation for the new network.
- Providing necessary network documentation.
- Providing ongoing support of the networks at the standby facility.
- Re establish the networks at the primary site when the post disaster restoration is complete.
- Ensuring the necessary security is put in place around the Data standby data centre
- Ensure that the environment changes go through the appropriate change management control.
- Provide regular updates to the DMT so they can update the client.
- Liaise and co-ordinate 3<sup>rd</sup> party providers to restore their services
- Put in place the necessary server infrastructure to enable the applications team to carry out application testing/restoration.
- Liaise and keep updated other parts of Serco who rely on services provided by ICT

### **3.3. Application Support CandI Team**

The Application Support CandI Team are responsible for planning for and assisting with the restoration of all applications in accordance with pre-defined RTO targets.

#### **3.3.1. Application Support CandI Team Responsibilities**

The Application Support CandI Team is responsible for the following

- Support restoration of all ICT Supported critical applications needed to satisfy the critical services recovery schedule.
- Assist in the application restoration, working with the Service Delivery Team
- Liaise with 3<sup>rd</sup> party application suppliers
- Ensuring that all documentation for standards, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate.
- Validate that all batch processes have been successfully restored
- Provide application testing where appropriate

### **3.4. Council / Facilities (Non-ICT)**

The Council is responsible for providing a fit for purpose environment to house ICT equipment and services. This facility must be capable of meeting the Space, Power, Air-conditioning, Security requirements, and connectivity requirements for a Standby Data Centre.

The Council will inform their staff of the processes they need to follow in the event of a Disaster Recovery situation being invoked.

The Council is responsible for all communications to their staff.

The Council will provide access to staff as required to assist with testing.

ICT will provide a small number of desktop and thin client devices into the area provided by the Council.

# 4. What to Do in the Event of a Disaster

The most critical and complex part of the management of resources is in the planning and organisation of the required personnel during the invocation of the plan.

Personnel must be well-rehearsed, familiar with the ICT Service Disaster Recovery Plan and be sure of their assignments.

## 4.1. Standard Emergency Procedures

**The first priority in a disaster situation is to ensure safe evacuation of all personnel.**

In the event of a major physical disruption, standard emergency procedures must be followed. This means immediately:

- Activating the standard alarm procedures for that section of the building to ensure that Medical, Security and Safety departments and emergency authorities are correctly alerted.
- If necessary, evacuating the premises following the laid down evacuation procedures and assemble outside at the designated location, if it is safe to do so.

## 4.2. The First Steps for the Recovery Teams

- The Council and ICT Disaster Management Teams assess the nature and extent of the problem.
- If it is safe to do so, the Service Delivery team performs an orderly shutdown of the Data Centre.
- The ICT Recovery Team is contacted and put on alert.

## 4.3. The Next Steps

The ICT Disaster Management Team decides whether to activate the ICT Service Disaster Recovery Plan, and which recovery scenario will be followed. Where there is no access to the Civic Offices this meeting may be held via a conference bridge.

The ICT Recovery teams then follow the defined recovery activities and act within the responsibilities of each team, as defined in this ICT Service Disaster Recovery Plan.

## **5. Recovery Scenarios**

This section describes the various recovery scenarios that can be implemented, depending on the nature of the disaster and the extent of the damage. The ICT Disaster Management Team Leader decides which recovery scenario to implement when they activate the ICT Service Disaster Recovery Plan.

### **5.1. Civic Offices (data centre or building)**

In this scenario, the entire Data Centre environment is out of action. Communication lines and the network, to and from the building, are out of action.

The goal of the recovery process in this scenario is to move all identified services and applications to the Standby Facility.

This scenario requires a full recovery procedure, as documented in this ICT Service Disaster Recovery Plan.

### **5.2. Derby Road Bridge - Grays**

In this scenario, the majority of Corporate Voice and Data network is out of action with no external power so the backup generators need to be activated

The goal of the recovery process in this scenario is to:-

- Recover external telephony numbers
- Recover WAN access to Civic Offices

Evaluation of the disaster recovery timescales will determine the need to migrate services to the Standby Facility.

### **5.3. Tasmania House - Tilbury**

In this scenario the Broadband network E2BN connectivity will be out of action, along with the CCTV concierge facility

The goal of the recovery process in this scenario is to:-

- Reconfigure the Broadband routing to cater for the loss of the Tasmania House node
- Reconfigure the Broadband routing to route Internet traffic via the Corporate internet pipe via Civic Offices
- Assist with the network requirements if the Concierge nominate a standby CCTV facility
- Establish a plan for re-connecting the Broadband network to E2BN (inc filtering etc)

## **5.4. ICT Resources**

In this scenario, the existing Pandemic BCP would be activated. These will be attached as part of the BCP pack.

# 6.Recovery Activities

This section contains a list of tasks for each of the recovery teams. Sensible judgment must be exercised to determine what activities are appropriate based on the nature and extent of the disruption. These timings are indicative and will vary depending on the exact disaster recovery scenario that needs to be addressed. In the event of a total loss of Civic Offices timescales will be significantly extended whilst a suitable Disaster Recovery site is sourced and capability established.

## 6.1. ICT Disaster Management Team Tasks

### 6.1.1. Immediate

- Assign a team leader
- Receive an initial assessment of the nature and extent of the problem.
- Agree with the Council whether to activate the disaster recovery plan.
- Alert all disaster recovery team leaders.
- Alert and mobilise all other team members.
- Setup a resource rota to ensure resources are utilised efficiently for 24hr working, if required.
- Make a preliminary (verbal) report to senior Council and Serco management.
- Call an initial meeting of the disaster recovery team leaders with the following objectives:
  - To define the problem, the extent of the ICT disruption, its consequences and the probable implications for the foreseeable future.
  - To set up a specified location as a Control Centre.
  - To agree each team's objectives for the next three hours.
  - To set up a second meeting for three hours later.
  - To open up a bridge line if required
- Make a second, more detailed, report to senior management on the content of the meeting and the actions being taken.

### 6.1.2. Within Three Hours

- Call a second meeting of the disaster recovery team leaders with the following objectives:
  - To receive initial reports from the recovery team leaders.
  - To take the decision to implement disaster recovery procedures.
  - To agree each team's objectives for the next twenty four hours.
  - To set up a third meeting for twenty four hours later.
  - Contact the supplier of the standby facilities to invoke the installation as per contract.
  - Contact 3<sup>rd</sup> party suppliers and inform them of the situation and arrange for the to assist as appropriate and source equipment

### 6.1.3. Within Twenty Four Hours



- Agree installation schedule with the supplier of the standby facility.
- Prepare plans for the transition to the standby facility.
- Make official declarations (for example, place of work change to any regulatory authorities).
- Report progress to senior management.

#### **6.1.4. Ongoing**

- Act as the main point of contact with the Council Disaster Management Team
- Monitor on a regular basis all activities to exercise and maintain control over delivery and installation dates.
- Document progress against agreed schedules
- Act as the main point of contact for the wider Serco Disaster Recovery team

## **6.2. Service Delivery Team Tasks**

### **6.2.1. Immediate**

- Attend the initial meeting called for recovery team leaders.
- Alert and mobilise all other team members.
- Inform non-core staff of what they need to do

### **6.2.2. Within Three Hours**

- Contact all Service Delivery and Application Support team staff.
- Inform all ICT staff of the problem and the actions being taken and their role
- Contact suppliers of:
  1. Hardware
  2. Communications equipment
  3. Ancillary equipment.
- Inform them of the arrangements for moving to the standby facilities.
- Order new equipment and arrange to have it installed in the standby facility.
- Report back at the second meeting of recovery team leaders.
- Contact Iron Mountain and organize the delivery of the required backup tapes
- Agree with the Council a stand down of all contractual SLA and KPI's

### **6.2.3. Within Twenty Four Hours**

- Accept hand over of standby site from the Facilities Team.
- Brief all operations staff required to travel to the interim site(s).
- In conjunction with the Service Delivery Network team, manage the procurement, delivery and installation of new/replacement hardware, communications and ancillary equipment.
- Inform all business contacts of the nature and extent of the problem, telling them that they will be kept informed of the plans to recover.
- In conjunction with the Service Delivery Networks Team, initialise and test the systems:
  - hardware

- operating systems
- communications network

#### **6.2.4. Ongoing**

- Call all business contacts on a regular basis, advising them of the disruption and the actions being taken. Initiate 'interim' back up procedures for priority systems (this may involve manual procedures) In the light of the disruption, review all production schedules in terms of jobs to be run, timings, priorities and dependencies. Prepare production schedules in readiness for start up at the standby site. Take security copies of all files and programs.
- Transfer security copies to off site storage location.
- Start processing in accordance with prepared production schedules.
- Discontinue work at any interim site(s).
- Keep a log of all changes that are required to bring services back online.
- Liaise with 3<sup>rd</sup> party suppliers

### **6.3. Application Support SandI Team Tasks**

#### **6.3.1. Immediate**

- Alert and mobilise all other team members.
- Attend the initial meeting called for disaster recovery team leaders.

#### **6.3.2. Within Three Hours**

- Contact relevant staff with a networks responsibility; inform them of the problem and the actions being taken.
- Ensure that all staff understands their roles.
- Inform networks staff of any temporary instructions.
- Help to compile an inventory of surviving communications equipment (voice/data) and that might be acquired.
- Ensure that all relevant documentation is at hand or retrieved from the off-site storage facility, for the reinstatement of the network.
- Liaise with the other parts of the Service Delivery Team as to the status of communications equipment and assist with acquiring replacement equipment if required.
- Ensure that all documentation/ information is available for the Service Delivery teams in order to connect the voice, local and wide area network to the standby facility.
- Liaise with the Standby Facility (if 3<sup>rd</sup> party) and telecom service providers to monitor progress of communications reinstatement.
- Report back at the second meeting of disaster recovery team leaders.

#### **6.3.3. Within Twenty Four Hours**

- Define the priorities for restoring the network on a gradual basis in order to provide a minimum initial communications requirement for normal operations.

- Liaise with suppliers of communications equipment to ensure prompt delivery, if required.
- In conjunction with the rest of the Service Delivery Team, ensure that the reinstated communications network is operable and tested.
- Provide ongoing support for the communications network and carry out any re configuration of the reinstated network that may be necessary.
- Attend the third meeting of the disaster recovery team leaders and report the restoration status.

#### **6.3.4. Ongoing**

- In conjunction with the rest of the Service Delivery Team, monitor the network's performance.
- Monitor, manage users' requests in the light of the restricted network.
- Prepare an inventory of all communications equipment requiring replacement in order for the original computer processing environment to be re utilised.
- Order replacement equipment as required.

### **6.4. Application Support CandI Team Tasks**

#### **6.4.1. Immediate**

- Alert and mobilize all other team members.
- Attend the initial meeting called for recovery team leaders.

#### **6.4.2. Within Three Hours**

- Contact relevant staff with an applications responsibility; inform them of the problem and the actions being taken.
- Ensure staff are informed and understand their roles.
- Inform staff of any temporary instructions.
- Ensure that all relevant documentation is at hand or retrieved from the off-site storage facility, for the reinstatement of the critical apps.
- Liaise with the rest of the Service Delivery Team as to the status of the application recovery and contact the suppliers where required
- Report back at the second meeting of recovery team leaders.
- Liaise with 3<sup>rd</sup> party suppliers

#### **6.4.3. Within Twenty Four Hours**

- Define or follow pre-agreed priorities. The priorities for restoring the applications on a gradual basis in order to meet the critical services recovery schedule.
- Liaise with suppliers to ensure prompt issue resolution, if required.
- In conjunction with the rest of the Service Delivery Team, ensure where feasible that the reinstated applications are operable and tested.
- Provide ongoing support for the applications and carry out any maintenance of the reinstated apps that may be necessary.

- Attend the third meeting of the disaster recovery team leaders and report the restoration status.

#### **6.4.4. Ongoing**

- In conjunction with the rest of the Service Delivery Team, monitor the applications performance.
- Monitor and deal with users' requests in the light of the restricted services.
- Continue to liaise with 3<sup>rd</sup> party suppliers until services are restored.

### **6.5. Facilities Team Tasks (ICT related)**

#### **6.5.1. Immediate**

- Provide an initial damage report to the Disaster Management Team Leader.
- Attend the initial meeting called for recovery team leaders.

#### **6.5.2. Within Three Hours**

- Provide the required space and facilities at the Command Centre.
- Provide the required space and facilities for the standby Data Centre
- Work with ICT and 3<sup>rd</sup> Parties, to install emergency comms.

# 7.The Command Centre

This section describes the Command Centre, from where the ICT Disaster Management Team will direct disaster recovery operations.

## 7.1. Primary Command Centre

If the Thurrock Council premises at Civic Offices are intact following the disaster, the ICT command centre will be located in the ICT area on the 3<sup>rd</sup> floor of CO2

## 7.2. Alternative Command Centre

If an alternative command centre is necessary, the command centre will be created by the Council in a venue to be defined.

## 7.3. Command Centre Requirements

<b>Item:</b>	<b>To be supplied by team:</b>
Data link to ICT Recovery Centre	Application Support Team
Network Switch / Firewall	Application Support Team
PC Workstations & Printer	Service Delivery Team
Telephones	Service Delivery Team
Power Backup – Generator / UPS	Facilities
Fax and Printer (MFD)	Service Delivery Team
6 Desks	Facilities

# 8. The Standby Facility

This section provides a general introduction to the standby facility which the Thurrock Council can utilise for a Data Centre following a disaster.

## 8.1. Location of the Standby Facility

The address of the Standby Facility is to be confirmed by the Council:

## 8.2. Standby Alert Confirmation Sheet (only for a 3<sup>rd</sup> party agreement)

The following form is used to confirm the invocation of the Standby Facilities. It must be completed by the ICT Disaster Management Team Leader and communicated to the Standby Facility Vendor.

**\*This section will be completed when a 3<sup>rd</sup> Party supplier is appointed**

Company Name:	
Address:	
Telephone Number:	
Disaster Alert Agreement Number:	
Designated Site:	
Nature of Disaster:	
Estimated Duration of Usage of the Standby Facility:	
Date Usage to Start:	
Name:	
Signature:	
Date:	

### **8.3. Standby Data Centre requirements**

This section provides detailed information on preparing the facility.

This information includes the following:

- 10MB Internet service - If Tasmania house is still functioning partial connectivity will be available via E2bN.
- 2 x Full height racks with 16amp commando
- Hardware see sun guard sheet \\Thurdata01\data\ICT\09-PROJECTS\02-ICT\_Projects\IPR0206 - ICT IT Service Disaster Recovery Plan\Supporting documentation\Sungard\DR Questionnaire Phase1+2.xls
- 2 x Small Air Con unit.
- 2 x 24port 2960 switches.
- 20 x desks with power.

The Service Delivery team will require access to a build area suitable for building and storing up to 25 PC's

## 9.The Data Storage Location(s)

This section describes the location(s) of the vault facilities where secure copies of data backups and other vital information are stored.

### 9.1. Backup Media

Location and address:	Iron Mountain
Contact person:	Terri Baglee – Account ID 0809
Contact phone number:	08445608020 - 07989533041
Reference:	“

### 9.2. DSL (definitive software library)

This specifies the location of all software that might be required for Disaster Recovery. These include applications and infrastructure (OS, AV, etc).

Location and address:	<a href="#">\\thurfiler01\dsl</a>
Contact person:	Gareth Moss
Contact phone number:	See Contact List
Reference:	



# 10. Critical Business Services

This section describes the requirements for Thurrock Council's critical business services in the Standby Facility. Phase 1 & 2 services are deemed by the Council to be the essential services, fulfilling their statutory obligations. (For the full list see appendix A).

It should be noted that the RTO targets are not achievable with the current DR capability. A standby Data Centre is required, with pre-existing network and equipment contracts in place in order to meet the timings below. Without this facility timings will be significantly extended.

## Critical Services – Phase 1 & 2

Phase	Area	Service	RTO
1	Infrastructure	Data room, power, air con, racks, security	Immediate
		ICT battleboxes	Immediate
		Servers, SAN, media backup drives	Immediate
		LAN, switches, routers	Immediate
		WAN corporate	Immediate
		WAN broadband (inc CCTV)	Immediate
		Internet access	Immediate
		PBX	Immediate
		User pc's	Immediate
		Backup media	Immediate
		Workshop + 20 pcs	Immediate
2	ICT Service Disaster Recovery plans	J: drive (BC & DR recovery documents)	12 hrs
		Outlook – essential users (not hist data)	12 hrs
2	Vulnerable people:	Careline – Council Responsibility	12hrs
		Home care CM2000 ... requires internet – Council Responsibility	12hrs
		ICS/IAS	7 days
		Saffron	7 days
	Deaths	Registrars	7 days
2	Financial	Bottomline	3 days
		Benefits payments SX3	3 days
		Cheque printing	3 days
		Oracle HR	1 week
		Oracle A/P	3 days
		PARIS	3 days
2	CCTV	Control centre	12hrs
		Streetlights	3 days
2	Public comms	Oracle CRM	3 days
		Express	3 days
		Website – Council Responsibility	3 days
2	ICT	ICT help desk - Phone contact	1 day
		ICT help desk – BMC Service Core	3 days
		Leapfile	7 days
		Workspace x 100 staff	7 days

# 11. Directories

This section of the plan contains a series of directories. These directories contain the type of information which is most likely to change such as names, addresses, telephone numbers etc. It is important to keep these directories up to date.

## 11.1. Recovery Team Members

The staffing of these Recovery Teams is listed in this section. The team leader is the first name in the list, in the shaded box.

### 11.1.1. Disaster Management Team: Members and Contacts

Removed from public version of this document

### 11.1.2. Service Delivery Team Members and Contacts

Removed from public version of this document

### 11.1.3. Service Delivery Networks Team: Members and Contacts

Removed from public version of this document

### 11.1.4. Application Support CandI Team: Members and Contacts

Removed from public version of this document

### 11.1.5. Council and Facilities Contacts

Removed from public version of this document

## 11.2. User Groups and Application Support

Removed from public version of this document

\*See Appendix A for the full Thurrock Service Listing

## 11.3. Vendor and Supplier Contacts

This section lists all the key vendors and suppliers who need to be contacted following a disaster.

Requirement	Contact/ Company	Phone /Fax (working hours)	Phone outside working hours	Contract no. if any
Standby Data Centre supplier	<i>tbc</i>			
Hardware – Server related	PDQ	01277 633533		
Hardware – Desktop related	XMA/HP			
Hardware – Network	Voyager / Cisilion	01344 420420		1907
	Cisilion	01372 201115		
Data communications	BT	0800 032 0025		
	Virgin / Telewest	01442 301184	07980 930990	627090701
	Cable & Wireless	01198216100		
	Networks by Wireless	0870 7077870		
	DUCL			
	Updata			
Voice communications	BT	0808 100 7499		

	Virgin / Telewest	0808 202 5436		
Cabling	Martin Allen	01255 431531	07918 889498	
	Extel	01375 395800	077970 434873	
Software	Bytes (Microsoft)	02087 861691	07943841867	
	B2 Net (VMware)	08442 488020		
Magnetic Media	Iron Mountain	08445 608020 / 07989 533041	08445 608020 / 07989 533041	Acc ID 0809

# 12. Inventories

This section contains inventories of all computer hardware, software and other equipment.

## 12.1. Computer Hardware

### 12.1.1. Servers

See [..\Supporting documentation\Sungard\DR Questionnaire Phase1+2.xls](#)

### 12.1.2. Network

See [..\Supporting documentation\Sungard\DR Questionnaire Phase1+2.xls](#)

### 12.1.3. Desktops/Laptops

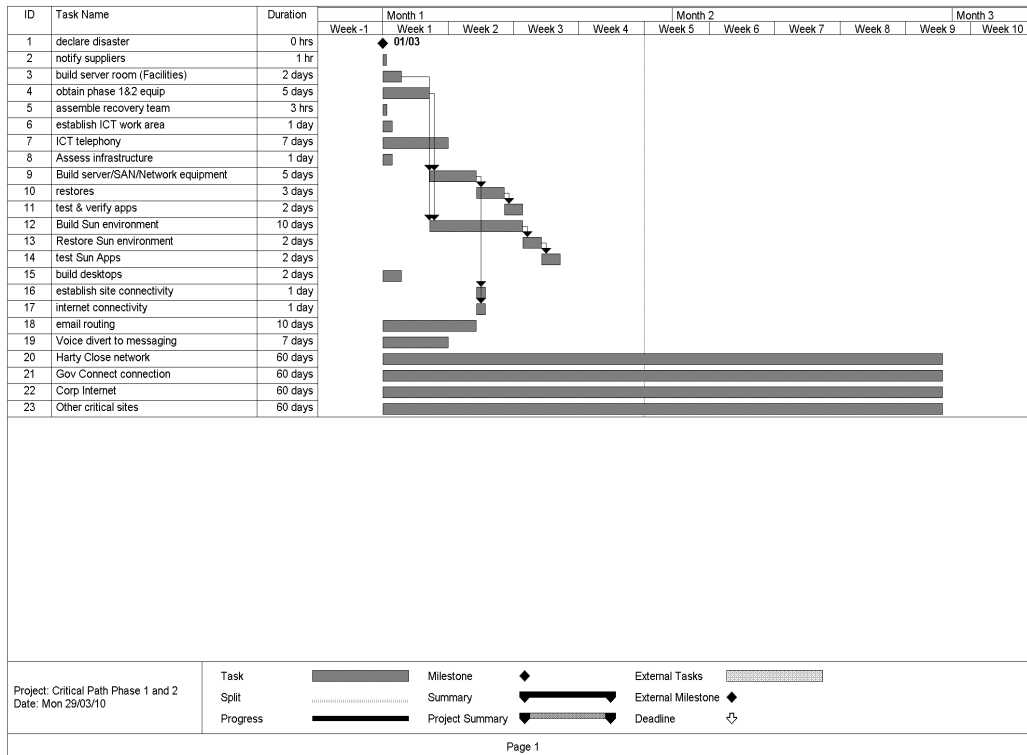
Any equipment needed will be provided by a third party or users having a laptop

### 12.1.4. Peripherals

In the event of a disaster an MFD device will be provided at the recovery location

# 13. Recovery Critical Path Plan

This section details the current Disaster Recovery schedule and dependencies.



This plan is assumption that an alternative facility is available immediately. In the event that equipment needs to be procured the timings could be delayed by up to 2 weeks.

# 14. Service Recovery Procedure list

This section lists the Recovery procedures for each Service. It also acts as a checklist

Service	Document	Owner
Data Centre - power, air con, racks, security	See section 8.3	Andy Best
ICT battleboxes		
Servers, SAN, media backup drives	Virtual Server DR Plan.doc Physical Server DR Plan.doc	Joe Gregory
LAN, switches, routers	Network Disaster Recovery.doc	Ray Caine
WAN corporate	Network Disaster Recovery.doc	Ray Caine
WAN broadband (inc CCTV)	Network Disaster Recovery.doc	Ray Caine
Internet access	Network Disaster Recovery.doc	Ray Caine
PBX	<a href="#">..\Supporting documentation\Telephony\DR Civic Offices.doc</a> <a href="#">..\Supporting documentation\Telephony\DR Concierge Tilbury.doc</a>	Bob Carr
User pc's		Andy Best
Backup media	Iron Mountain - Request Media Delivery via SecureSync.doc	Joe Gregory
Workshop + 20 pcs		Andy Best
J: drive (BC & DR recovery documents)	Virtual Server DR Plan.doc	Joe Gregory
Outlook	Bare-Bones Exchange Server DR Plan.doc	Joe Gregory
Careline		Council
Home care CM2000 ... requires internet	<a href="#">DRP - Applications - CM2000.doc</a>	Gerry Waterfield
ICS/IAS	<a href="#">DRP - Applications - ICS_IAS.doc</a>	Gerry Waterfield
Saffron	<a href="#">DRP - Applications - Saffron.doc</a>	Gerry Waterfield
Registrars	<a href="#">DRP - Applications - Registrars.doc</a>	Gerry Waterfield



Albacs	<a href="#">DRP - Applications - ALBACS.doc</a>	Gerry Waterfield
Benefits payments SX3	<a href="#">DRP - Applications - Benefits Payments Sx3.doc</a>	Gerry Waterfield
Cheque printing	<a href="#">DRP - Applications - Cheque Printing.doc</a>	Gerry Waterfield
Delphi - Payroll	<a href="#">hrdelphidisas.doc</a>	Gerry Waterfield
Oracle A/P	<a href="#">DRP - Applications - Oracle Financials &amp; CRM.doc</a>	Gerry Waterfield
PARIS	<a href="#">\DRP - Applications - PARIS.doc</a>	Gerry Waterfield
Control centre		Gerry Waterfield
Mayrise	<a href="#">DRP - Applications - Mayrise.doc</a>	Gerry Waterfield
Oracle CRM	See Oracle A/P Above	Gerry Waterfield
Express	<a href="#">DRP - Applications - Express.doc</a>	Gerry Waterfield
Website - Intranet	Physical Server DR Plan.doc	Gerry Waterfield
Website External	Externally Hosted	
ICT help desk - Phone contact		Andy Best
ICT help desk - BMC Service Core	DRP - Applications - Footprints.doc	Andy Best
Leapfile		
Workspace x 100 staff & PCs		Council

# Appendix A

Phase	Area		RTO	Who	Comment
1	Infrastructure	Data room, power, air con, racks, security	Immediate	facilities	Temporary or permanent facility? Need to source
		ICT battleboxes	Immediate	ICT	Recover
		Servers, SAN, media backup drives	Immediate	suppliers + TS	Need to source - phase
		LAN, switches, routers	Immediate	suppliers + TS	Need to source - phase
		WAN corporate	Immediate	suppliers + TS	Need to source
		WAN broadband (inc CCTV)	Immediate	suppliers + TS	Need to source
		Internet access	Immediate	suppliers + TS	Need to source
		PBX	Immediate	suppliers + TS	Need to source, Need to redirect at exchange
		User pc's	Immediate	suppliers + SD	Need to source (25 in Culver) - phase
		Backup media	Immediate	supplier	Recover from offsite storage - phase
	Workshop + 20 pcs	Immediate	facilities	Need to source	
2	ICT Service Disaster Recovery plans	J: drive (BC & DR recovery documents)	12 hrs	TS	critical biz continuity docs only ICT DR plans ... store on remote laptops for quick recovery
2	Vulnerable people:	Outlook	12 hrs	TS	Not normal operating accounts
		Careline	12hrs	suppliers + business	elderly people management, externally supplied
		Home care CM2000 ... requires internet	12hrs	supplier + AS	elderly people management
		ICS/IAS	7 days	supplier + AS	Vulnerable people DBs: ICS/IAS
	Saffron (+ Jacada)	7 days	supplier + AS	to re-home people in vacant properties	
	Deaths	Registrars	7 days	TS + SD	Internet connectivity
2	Financial	Albacs	3 days	supplier + AS	Suppliers will still need paying

		Benefits payments SX3	3 days	supplier + AS	
		Cheque printing	3 days	supplier + AS	Suppliers will still need paying staff will still need paying
		Oracle- Payroll	1 week	supplier + AS	
		Oracle A/P	3 days	NW + AS	
		PARIS	3 days	supplier + AS	to take payments
2	CCTV	Control centre	12hrs	suppliers + TS	
	Streetlights	Mayrise	3 days		
2	Public comms	Oracle CRM	3 days	NW + AS	
		Xpress	3 days	supplier + AS	in election years
		Website	3 days	suppliers + business	externally supplied
2	ICT	ICT help desk - Phone contact	1 day	SD	
		ICT help desk - Touchpaper	3 days	TS + SD	
		Leapfile	7 days	TS + SD	
		Workspace x 100 staff	7 days	SD	Need to source - PCs, handsets, printers & build Follow facilities with desks or remote working
3	Applications	Business Objects	14 days	supplier + AS	Universe sequence
		ControCC	14 days	supplier + AS	
		Oracle - HR	14 days	supplier + AS	
		FMS	14 days	supplier + AS	
		Full - Outlook	14 days	TS	
		ICPS	14 days	supplier + AS	
		Igneous	14 days		
		Information@Work	14 days	supplier + AS	
		Oracle A/R and G/L	14 days	supplier + AS	
		TRACE	14 days	AS	
		Uniform	14 days	supplier + AS	
	ICT	Web serving	14 days	TS	

	Workspace x 100 staff	14 days	SD	Need to source - PCs, handsets, printers & build Follow facilities with desks or remote working
4	Applications	Apex	21 days	supplier + AS
		ESRI	21 days	supplier + AS
		GIS	21 days	supplier + AS
		Igneous	21 days	supplier + AS
		J: drive	21 days	TS
		Objective EDRMS	21 days	supplier + AS
		SIMS	21 days	supplier + AS
		Symology	21 days	supplier + AS
	ICT	Tribal suite	21 days	supplier + AS
		Workspace x 100 staff	21 days	SD Need to source - PCs, handsets, printers & build Follow facilities with desks or remote working
5	Applications	Avco Anycomms	28 days	supplier + AS
		CMIS	28 days	supplier + AS
		Databox	28 days	supplier + AS
		Debtco	28 days	supplier + AS
		Eforms	28 days	supplier + AS
		Express	3 days	supplier + AS
		Transform	28 days	TS
		H: drive	28 days	TS
		InPhase	28 days	supplier + AS
		ITTD	28 days	supplier + AS
		Netloan	28 days	supplier + AS
		Planning portal	28 days	supplier + AS
		Softsmart	28 days	supplier + AS

Non-election years

	Statement tracking & Welfare	28 days	Essex + AS	
	Total Land Charges	28 days	supplier + AS	
	Vubis	28 days	Essex + AS	
	Warrior	28 days	supplier + AS	
	Y: drive	28 days	TS	
	YOIS	28 days	supplier + AS	
ICT	Workspace x 100 staff	28 days	SD	Need to source - PCs, handsets, printers & build Follow facilities with desks or remote working
Unsupported applications	Across		User	
	Asset register		User	
	AURN		User	
	CASPA		User	
	CBL		User - Ext service	
	COLLECT		User	
	ContactPoint		User - Ext service	
	Coop financial director		User	
	Datamap		User	
	Dreamweaver MX		User	
	EPAS		User	
	eRoom		User - Ext service	
	FFT		User	
	FIS Module		User	
	Galaxy		User	
	Ichis		User	
	ID PRO		User	
	IFD RPMS		User	
	Insight		User	
	Insight enterprise		User	
	IPFasset manager		User	
	Key to Success		User	

Keypas	User
LAIT	User
LARA	User
Logotech	User
NAPTAN 2	User
NCCIS	User
Netmedia suite	User - Ext service
Novalet	User
Ofsted profile	User
OnPoint	User
PDA	User
Performance plus	User
Registrars	User - Ext service
Respond	User
Riase online	User - Ext service
RON	User
RSS	User
SAT admin	User
School Transport Manager	User
School-to-School	User - Ext service
SPOCC	User
SR3	User
Supporting people	User
System K	User
Target tracker	User
TellUs	User
The Hub	User
TOPIC	User
TransoniQ	User
VIP	User

