Community Relations Council

Northern Ireland Community Relations Council

Service Continuity Plan

April 2017

Document Control

The Current status of the document is issued Final.

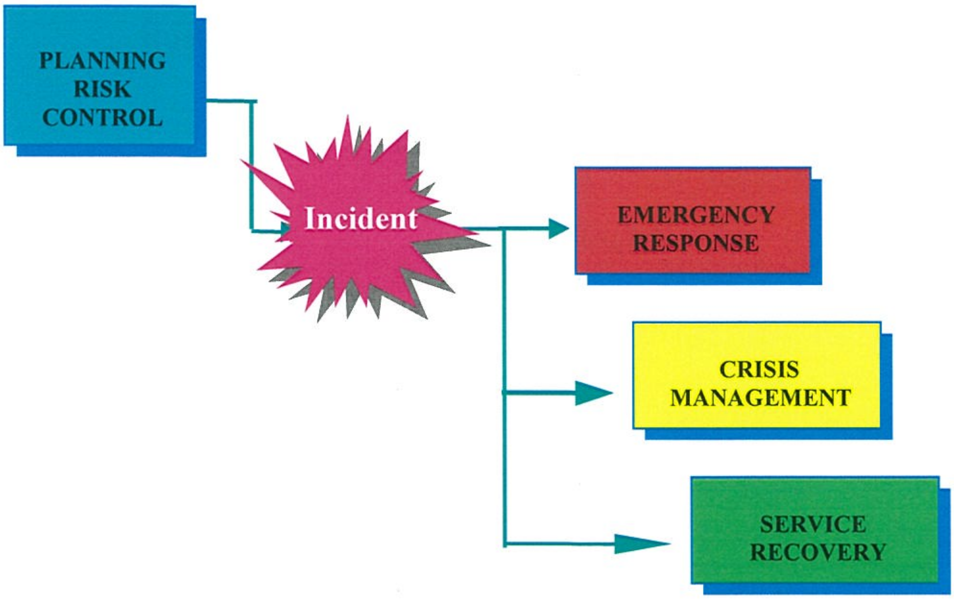
Version No.	Approval by	Approval date	Issue date
ONE		22nd February	7-3-18

INTRODUCTION

1.1. The Service Continuity Plan

This Service Continuity Plan [SCP] provides overall guidance to the Management in responding to any significant incident that threatens to interrupt normal operations. It works at the **worst loss** level and for less severe incidents, only the relevant sections of the plan would be selected.

The full plan is set out in three time-phased categories and is focused on assisting the Senior Managers with the handling of the issues that will arise after an incident has occurred. This is illustrated as follows:



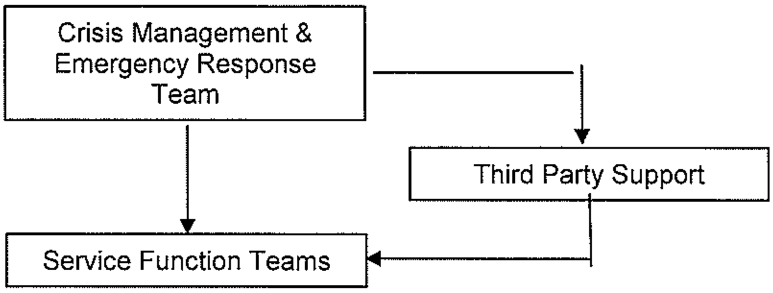
The central feature of the plan is a section of colour coded pages, covering the entire post-emergency response from the initial emergency through to the resumption of normal or near-normal operations.

The key actions that may need to be performed and the key issues that are likely to arise are summarised. The pages are designed to act as checklists, helping to ensure that no major actions or issues are neglected.

A variety of procedures, guidelines and contacts, in support of these checklists, are included in the plan.

1.2. Major Incident Command and Control Arrangements

The Command and Control arrangements in managing a Major Incident can be graphically shown as follows:



Because the Community Relations Council is a relatively small organisation the short and longer term management of the response to a major incident will be handled by the same team called the CMERT.

POLICY STATEMENT

The Community Relations Council has developed this Service Continuity Plan to ensure that operations are conducted with the highest regard for both the safety and health of our employees and the public, the continuation of the highest quality service to our clients, and the protection and preservation of property and the environment.

The Service Continuity Management Plan encompasses the areas of health, fire protection, environmental control, security, training, public affairs, communications, quality control, maintenance and operations. The plan is designed to mitigate the effects of and recover from a range of credible or potential emergencies/disasters within the organisation.

The Service Continuity Plan is a description of our overall emergency response arrangements. It designates responsibilities and describes notification procedures necessary to cope with serious interruption to normal business. It aims to provide for effective response and rapid recovery and will help the organisation to protect as far as is possible our human and material assets.

Signed by: Date:

Jacqueline Irwin
Chief Executive Officer

Distribution List

Title	Name	Work	Mobile
The Chair	Peter Osborne	02890 227500	07803717930
Chief Executive Officer	Jacqueline Irwin	02890 227500	07734044747
Director of Finance, Administration and Personnel	Gerard McKeown	02890 227500	07943244402
Director of Community Engagement	TBC	02890 227500	TBC
Director of Funding and Development	Paul Jordan	02890 227500	07788882199
Human Resources Manager	Jo Adamson	02890 227500	07762512113
Performance Management manager (ECNI)	Frank McWilliams	02890 500 600	07879438904

Access to Plans

The Crisis Management & Emergency Response Team (CMERT) members must keep copies of their plans readily available at all times. As minimum copies are to be kept at two or more of the following options:

- In the office (to take out on evacuation)
- In the car
- In a briefcase
- At home (by the telephone).

The CMERT will:

- Provide strategic direction in relation to a major incident
- Agree necessary resources
- Manage media interest and inform customers of any loss of service

INCIDENT DEFINITION

Within the framework of the Service Continuity Plan an incident requiring a Service Continuity response is defined as any event that:

1. Prevents any of our Divisions, from continuing with their normal service functions, as a result of a genuine threat to:

   - Site,
   - Facilities,
   - Utilities, or
   - Human life

2. Falls outside the scope of normal service contingencies for managing Division and site interruptions.

An incident will only require the invocation of the Service Continuity Plan if it is of a very serious nature.

Below is a list of the types of incident that may require a Service Continuity response.

Natural	Description of incident
Explosion	Explosion in CRC Offices or in back up facility with severe damage to site
Fire	Fire in CRC Offices or in back up facility with severe damage to site
Water damage	Water damage resulting in severe damage to site
Human	
Unnatural death	Unnatural death of staff member, client or member of the public on premises
Contamination	Contamination of site by infection or deliberate act of terrorism
Loss of key staff	Immediate or longer term loss of key people – CEO and the Chair
Technical	
Power failure	Failure resulting in loss of IT systems

INVOKING THE PROCEDURE

Any *two* members of the CMERT can invoke the Service Continuity Plan.

In so doing, the CMERT will decide whether to authorise the invocation of the Service Continuity Plan in part or in full.

Issues to consider:

A Has the incident devastated the premises? - the Service Continuity Plan will be invoked immediately;

B Is the damage to the site only partial? – at least two members of the CMERT should go to the site and report on the extent of the damage and potential unavailability period in the first instance before the plan is invoked.

C Is there denial of access not associated with physical damage to the premises? - further information is likely to be sought by the CMERT before a decision is made.

Refer to the agreed incident definition as a guide on the relevance of the Service Continuity Plan as the response to the incident.

RECOVERY STRATEGY

In the event of a denial of access to our facilities, the strategy for managing the crisis and recovering the organisation is based upon the overriding objectives of:

1. protecting personnel;
2. controlling the threat;
3. securing the site;
4. protecting assets; and
5. managing the media.

The strategy for recovering the service once these objectives have been achieved will be:

1. To communicate effectively with staff
2. To set up alternative contact arrangements for clients
3. To obtain alternative working premises
4. To establish working IT and recover data

The strategy for managing the crisis and recovering the organisation is based upon

- the actual steps, people and resources required to recover critical processes and data;
- Defining staff and IT alternatives;
- Defining alternative sources for critical functions;
- Obtaining an alternative location;
- Planning transition back to normal operation;
- Communicating effectively with staff;
- Setting up alternative contact arrangements for clients and key stakeholders

REVIEWING THIS PLAN

This plan must be reviewed every 12 months and updated accordingly; the plan must be re-issued to those on the Distribution List within 4 weeks of the review. If the 6 monthly review reveals no changes are required, those on the Distribution List should be so notified.

The review of the plan is the responsibility of the Audit and Risk Assurance Committee, and will form part of the documentation reviewed by the Internal Audit function. The Management Team must fully support this plan and a note of the review must be recorded in the Management Team minutes.

Version	Date Tested / Amended	Sections Tested / Amended	Tested / Amended By

The Distribution List will be updated should there be a change in post holder on the CMERT by the HR Manager and circulated to members of the CMERT.

Emergency Response	Summary

Emergency Response Phase:

This phase covers the first minutes and hours following the incident and the immediate actions that are likely to be required.

The phase covers:

- Evacuation
- Roll call
- Emergency service call out
- Attendance to injured
- Missing persons search
- Site shut down
- Securing the site
- Damage assessment

Key procedures

In support of the tables, there are special procedures for the following type of incident:

Action	Procedure	Responsibility
Evacuation	Evacuation procedure	Officer Evacuation Officer – Jo Adamson
Emergency Services Call out	Evacuation procedure	Officer Evacuation Officer – Jo Adamson
Use of Evacuation Chair	Evacuation procedure	Officer Evacuation Officer – Jo Adamson
Roll Call	Evacuation procedures	Manager HR
Attendance to injured	Health and Safety Procedure	CRC First aiders
Missing Persons search		Emergency services
Site shut down		Emergency Response Team

Rendezvous Points

Pre agreed reception points for the ERT have been identified as:

Assembly Points	Roll Call Supervisor at point
Posnett Street Car Park.	HR Manager
Other as notified by security forces in event of a bomb threat.	HR Manager

CMERT

CMERT Team co-ordinator: Jacqueline Irwin

Receive advice of situation / information
Call out at least two members of the CMERT Team and agree to meet at rendezvous point
Liaise with the Emergency Services & Security
Make an initial assessment of the situation
Meet up with CMERT Team leader at agreed rendezvous point - establish common understanding
Call out rest of CMERT Team and brief members
Refer any media enquiries to Head of Engagement
Initiate instructions to all Management and Staff

CMERT Team Members

Receive advice of situation / information
Start a log of actions taken
Call out at least two members of the CMERT Team and agree to meet at rendezvous point
Liaise with the Emergency Services & Security
Start a log of actions taken
Make an initial assessment of the situation
Meet up with CMERT Team leader at agreed rendezvous point - establish common understanding
Call out rest of ER/ CM Team and brief members
Refer any media enquiries to Head of Communications & Learning
Initiate instructions to all Management and Staff
Decide on Course of Action
Communicate decision to staff and stakeholders
Set up Command Centre
Provide public information to protect reputation and business
Consider immediate actions to be taken by specialist staff - IT, HR, etc
Decide what to do with staff in the short term
Brief managers to instruct staff to return to work or go home
Attend to any problems arising from: • loss of cash • loss of car keys • denial of access to cars • loss of personal effects
Ensure that all staff have been accounted for.
Arrange a debriefing session and start the completion of incident report form (see Page 10)

Emergency response	**Incident Report Form**

Summarise the situation on this form as at ……. Hours, Date…………………………..
A fresh form may be required as the situation becomes clearer and at periodic intervals.

Questions	**Done by**	**Record information in this column**
What has happened e.g. fire, explosion, theft, malicious damage, water damage, power failure, denied access, staff availability problem?		
Have emergency services been called		
Who is in charge of the situation? ❑ Police ❑ Fire and Rescue service ❑ Local Manager or other member of staff		
Any casualties: • any injury reports • any staff, visitor or contractor injuries or fatalities • where are staff now? – evacuated, or not • have Incident services (fire, police, ambulance) / local authority been called?		
When did / will it occur?		
Where is the problem?		
What is the extent of the problem? General indication of the extent of the impact, or area affected (if known).		

What is the state of services and utilities? □ Electricity □ Water □ Gas □ Telephony/switchboard □ ICT		
Why did it happen? If known at this stage.		
Who knows about the situation so far? Who else needs to know?		
Are there any further threats?		
Notes:		

Crisis Management

Plan Activation

The Crisis Management Phase is only activated where the situation demands and is designed to ensure that actions are taken to minimise, as far as possible, the effects of the major incident or emergency situation and ensure timely and effective management of service recovery. It builds upon the emergency response and will overlap the ongoing activity of those involved in the emergency response phase.

The decision to activate this phase of the plan rests with the CMERT Leader or the Deputy Team (CMERT) Leader.

The decision will be based on:

- the scale of the disruption
- the loss of life or serious injury

The CMERT will:

- provide strategic direction in relation to a major incident,
- agree necessary resources,
- manage the media and maintain our reputation.

Command Centre

The Command Centre will be occupied following the initial emergency response and the CMERT will act as the co-ordination point for the efficient and speedy allocation of resources to ensure a return to normal operating conditions.

Location and immediate action set up details are shown overleaf:

CRISIS MANAGEMENT	**COMMAND CENTRE**

Impact	Location	Contact	Address	Telephone No.	Email Address
Loss of Community Relations Council office space	Board Room – Equality House	Frank McWilliams	7-9 Shaftesbury Square Belfast BT2 7DP	02890 500 600	FMcWilliams@equalityni.org
Loss of Building	NI Screen	Linda McGuiness	3rd Floor Alfred House, 21 Alfred Street, Belfast BT2 8ED	028 90268 591	LindaMc@northernirelandscreen.co.uk

Immediate Action Set-up Details

- Set up telephones and fax machines.
- Set out desks in a suitable manner to enable personnel to be close enough to be aware of events as they unfold but not too close to hinder the ability to operate and use the telephones.
- IT Assistant to contact IT Service Provider to provide temporary IT system
- Set up TV / video, audio-visual equipment if available.
- Organise rota system to man Command Centre (check if 24 hour cover is needed).
- Organise refreshments / food.

Notify Employees

- Notify all employees of the emergency situation. Some of the employees will be requested to report to the emergency operations site immediately and some will be requested to come later

- Request all employees associated with business functions requiring resumption in 3 days or less to report to the emergency operations center.

- Use the “Key Employee List - Sorted by Notification Order” information sheet and call starting with the first key employee until the activation time of the employee is greater than 3 days.

- Inform all other employees to remain available for activation within 24-48 hours.

Retrieve and Restore Selected Systems & Backup Sets

Retrieve and restore backup media of all backup sets required for support of business functions whose recovery time is 3 days or less. Use the "Backup Sets - Sorted by Recovery Requirement" information sheet.

Notify Key Customers and Vendors As Required

Use the information sheets listing vendors and key customers as a checklist for calling customers and vendors as necessary and desirable depending upon the specific emergency situation.

Crisis Management Events

Sequence of events	***Date/time***	***Event***	***Point to note***	***Note 1***	***Note 2***	***Note 3***
Damage	Item	repairable	replace	supplier	Contact number	Cost £
Running outstanding action list	issue	Who contacted	Contact name	Contact Tel/fax		
Casualties	name	Employee Visitor Contractor public	Nature of injury	Name of hospital	Next of kin	Contact made, time & date
Hot spots	Date / time	Issue	Action to date	Contact names	Contact Tel & fax no	
Relatives	Date / time	enquiry	Action to date	Contact names	Contact Tel & fax no	
Media	Media enquiries / briefings and interview bids	Name of paper/radio/ TV station	Contact name	Contact Tel & fax no	Media statement sent to	
Suppliers	Date / time	Order placed / issued	Action to date	Estimated delivery date	Contact name	Contact Tel & fax no
Expenditure authorisation	Date / time	Item	Value			
Expenditure incurred	Date / time	Item	Value £ cheque	Value £ cash	Value £ credit card	

CRISIS MANAGEMENT	**Tasks and Responsibilities**

The CMERT should take responsibility for the following tasks and delegate as required:

Strategic Management

Go to the agreed Command Centre
Receive report on the incident from a designated person remaining at site
Decide whether to activate the Plan
Support the designated person at site in decisions affecting the recovery
Inform The Executive Office
Liaise with the person responsible for Media Handling (Director for Finance, Administration and Personnel)
Receive damage assessment reports from the designated person at site
Consider impact on our activities
Inform and liaise with the Enforcing Authorities
Ensure Management and Staff are kept fully informed and up to date with progress
Receive progress report on recovery activities
Review and adjust recovery strategy as necessary
Seek update on longer term reinstatement plan

Media Handling

Manage media interest
Consider use of a press release - in conjunction with Emergency Authorities
Double check to ensure that a consistent message is being given
Inform media about channels for information
Liaise with CMERT for press conference facilities/web site update
Revise media statement
Maintain awareness of changing emphasis of interests

Human Resources

Obtain injury and missing persons reports from the First Aiders and Fire Wardens
Send representatives to hospital
Provide Next of Kin list to Police
If appropriate set up an emergency number for welfare issues
Assist in obtaining re-location transport for staff
Arrange hospital visits
Arrange trauma counselling as appropriate
Develop support for relatives
Assess staff morale and assist as necessary

Support on-going process of staff relocation/relocation costs
Support staff at home as necessary
Contact recruitment agencies if required

Finance/Administration

Sanction and draw up lists of costs incurred by recovery teams
Draw up schedule for monies due/payable
Consider overall finance needs and seek The Executive Office assistance
Work with Insurers and loss adjusters

Facilities Management – Alternative Location

Assess premises needs with The Executive Office
Organise alternative accommodation for Departments with immediate needs
Identify likely timescales for alternative premises
Take possession of the new premises
Arrange for services/fitting out to be done - contractors and specialists
Arrange for supplies to be diverted
Hand over to the IT team
Arrange for electro/mechanical installations

Telecommunications

Arrange for immediate divert of critical lines
Establish what is working and salvageable
Arrange for contractors to reinstate switches/network (if possible)
Set up temporary arrangements for voice mail and email
Segregate damaged equipment for repair
Organise specialist cleaning
Maintain records of costs incurred
Re-configure telecom systems
Load backed-up system data and test
Plan layout & specification of temporary/permanent location
Build up new telephone extension numbers
Resolve network problems reported
Advise Departments as networks go live
Recommence daily back ups & off-site storage

Information Technology

Control shut down of systems
Conduct assessment, salvage possibilities and systems unavailability
Invoke IT Contingency Plan and procedures
Liaise with specialist service providers
Ensure security of data and equipment

Segregate damaged equipment for repair
Organise specialist cleaning
Maintain records of costs
Collect back- ups of data held off site
Restore some level of service
Plan layout & specification of temporary/permanent location
Build up workstations
Rebuild data network
Advise departments as they go live
Recommence daily back-ups & off site storage

Designated Person at Site

A designated person will be at the site of the incident already and may move from their temporary rendezvous point to join the CMERT in the designated Command Centre.

This person will fulfil the following support / infrastructure tasks to recover our activities as appropriate.

In practical terms the Heads of Departments would call upon their own staff to provide specialist assistance.

Facility Management at the damaged site

Ensure Health and Safety as a priority
Liaise with landlord to assess damage
Liaise with landlord and security to ensure protection of undamaged equipment and work areas
Photograph damaged areas, if possible
Advise the CMERT on the potential period of unavailability of the premises
Meet Loss Adjusters on site
Call out clean up/salvage/restoration contractors, if appropriate
Arrange commencement of temporary repairs
Liaise with landlords to arrange temporary light, power, heat, etc
Commence salvage activities
Re-direct mail
Work with consultants in quantifying repair needs
Oversee works
Liaise with landlord re cleaning/chlorinating water supplies before re-occupying
Commission electro/mechanical installations
Arrange for services (gas, electricity, water) fitting out to be done
Commission IT and Telephone installation

Service Function Recovery

The directors of business functions immediately impacted by a major incident should do the following:

Assess known effect on your Division and list immediate needs
Decide with CMERT what activities can be suspended or alternative actions to be initiated.
Establish one person to act as the liaison co-ordinator with all other teams
Consider impact of the disruption on clients and the public
Update managers and assist in detailed communication to staff
Establish limited working as soon as possible - as enabled by the CMERT
Establish if any work in progress / work materials have been lost
Re-appraise priorities
Review & adjust recovery strategy
Work with HR to identify staffing needs
Reschedule work

Designated Person at Site

A designated person will be at the site of the incident already and may move from their temporary rendezvous point to join the ERT in the designated Command Centre.

This person will fulfil the following support / infrastructure tasks to recover our activities as appropriate.

In practical terms the Directors would call upon their own staff to provide specialist assistance.

Backup Strategy

The issues and items listed in this section of the plan should reflect the requirements of each individual Department or organisation function. Any item that a Department has identified as essential should be included as part of the backup strategy.

CRISIS MANAGEMENT	Contingency Box – Off-Site Items

Virtual Contingency Box Stored on secure folder on ECNI Server

Location:	Virtual folder on server
Maintained by:	Director of Finance, Administration and Personnel

Owner	Description of item
DFAP	1. Business Continuity Plan
HR	2. Emergency contact details for staff
CRC IT	3. ICT Asset Register and Inventory
Finance	4. Other Assets Register and Inventory
HR	5. Paper copies of Personnel - addresses and next of kin
ECNI IT	6. ICT documentation re. systems, maintenance agreements for hardware / software etc
CRC IT	7. IT SLA Documentation
ECNI IT	8. Restoration procedures
CRC IT	9. Website contact details
ECNI IT	10. ICONI contact details and access procedures
Finance	11. Letterheads, paper and compliment slips
HR	12. Procedures Manuals
DFAP	13. Copies of current Corporate Plan and Business Plan

Data Protection

In order to comply with Data Protection and financial procedures, the Contingency Box will password protected and any sensitive personal information locked and stored securely.

CRISIS MANAGEMENT	Off-Site Items List

Location:	NI Screen
Maintained by:	ICT

Contents in each location	No.	Comment	Confirmed
Personal Computer	1	CMERT members provided with laptops with VPN access	
Telephones	1	Key individuals in ERT have been provided with secure smart phones. Others will use personal mobile phones	
Internet connection	1	Available via ECNI. VPN provides secure login to servers via any WIFI	
Printer	1	Access to be provided on site	
Photocopier	1	Access to be provided on site	

CRISIS MANAGEMENT	CALL DIVERT PROCEDURE

PROCEDURE TO BE FOLLOWED TO ESTABLISH A RECORDED MESSAGE ON ALL INCOMING VOICE LINES

The main lines i.e. 02890 227500 and 02890 227501(fax) would be rerouted to two Temporary lines within the Command Centre. A temporary reception would be established to field calls and take messages within 24 hours of disaster.

PROCEDURE TO BE FOLLOWED TO DIVERT TELEPHONES

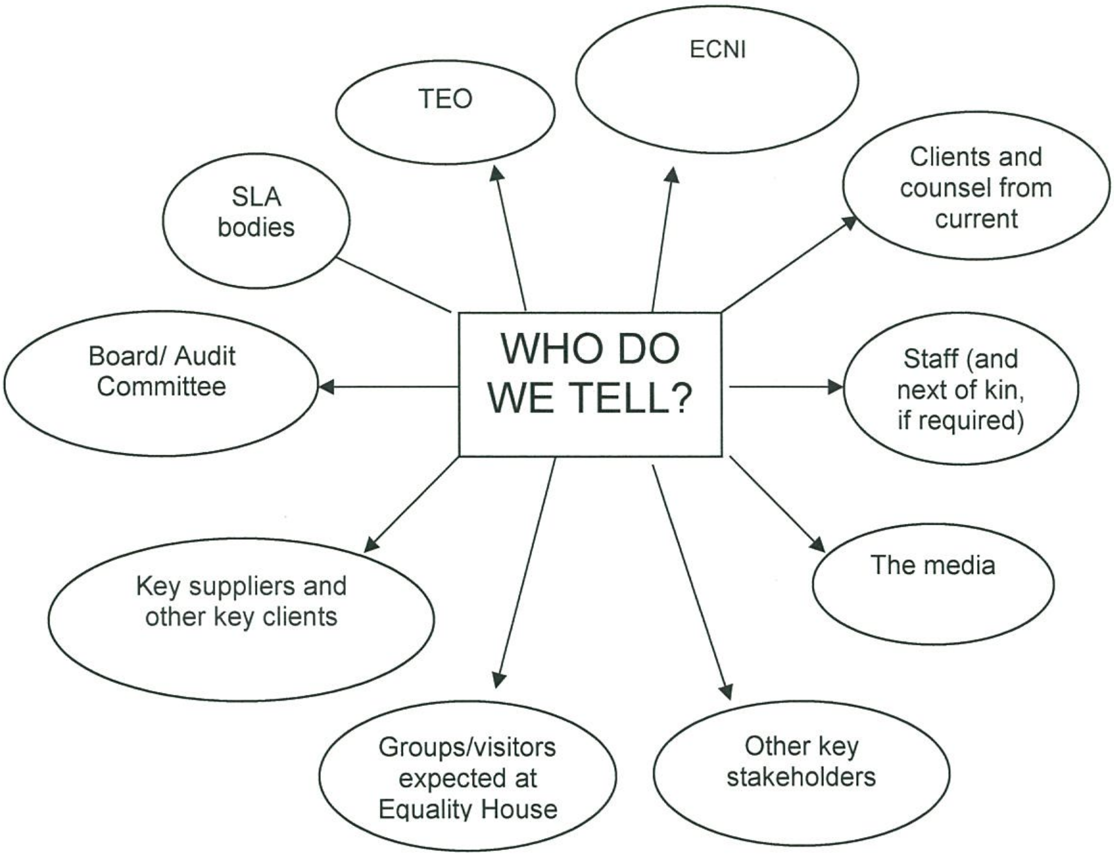
- Contact BT 24 hour Service outage centre

0800 800 212 Account No for 02890 227500
VP 26089370

CRISIS MANAGEMENT	**DAMAGE REPORT FORM**

Form completed by:		**Contact number:**		
Date and time of incident:				
Incident description	Type of incident			
	Cause (if known)			
	Areas of site affected			
Physical damage (excluding IS/Telecoms)	Buildings			
	Machinery			
	Utilities			
IS/Telecoms damage	Hardware (main)			
	Hardware (peripheral)			
	Telecoms			
	Network			
Initial estimate of site restoration		Operations	IT	Admin
	Less than 1 week			
	1 week – 1 month			
	1 – 4 months			
	Over 4 months			

Critical to the maintenance of our reputation while recovering from an incident is the need to inform key stakeholders. The following is a useful aide memoir:


WHO DO WE TELL?
TEO
ECNI
SLA bodies
Clients and counsel from current
Board/ Audit Committee
Staff (and next of kin, if required)
Key suppliers and other key clients
The media
Groups/visitors expected at Equality House
Other key stakeholders

CRISIS MANAGEMENT

Communications Checklist

To be used in conjunction with the preceding communications guidelines.

Who?	By Whom?	When?	What was said?

Media Golden Rules

Buy Time / Be Prepared

- Never speak to media without a management briefing from Communications staff.
- Always seek to delay the process - work to your timescales - structure your commitments e.g. statements / interviews will be at 2pm and 5pm - ration your time.
- If a surprise interview is requested, delay it, if possible, even by 5 minutes.
- Establish the type of issues they want answered ahead of time so you can prepare suitably.
- Speak with as much preparation completed as possible.
- Prepare key points you want to say and if the first question does not give you the opportunity to give that message, start with ‘ before I answer that question, may I say “.......”

Remember

- Facts are key - Assume nothing.
- Avoid “no comment” responses - it suggests the worst.
- Deception is fatal.
- Doubts destroy confidence = conjecture about dishonesty = the conjecture will develop into firm belief that there is dishonesty - there is a need for a firm denial.
- Someone else will be telling the story without correct information and their version sets the mood.
- People will feel privileged if told early enough and are trusted with the facts; they will feel disillusioned if they ‘discover’ the truth; they will become disaffected if their story differs from yours.
- Answer everything and understand they suffer too.
- Manage and control the flow of information.
- Media priorities are **people, environment, property and money**

Show:

- Concern - you care about what has happened - this is the most important fact.
- Commitment - to find out what happened and put it right.
- Control - of situation at most senior level.

DO'S

- Be positive and truthful.
- If you do know - tell them, if you don't know - tell them you don't know.
- Do not speculate - instead defer to the enquiry to follow.
- Remember - you want the answers more than anyone else.

DON'TS

- Admit liability – refer to the need for the matter to be fully investigated.

SERVICE RECOVERY	RECOVERY PRIORITIES

A target recovery time frame has been established for all of the organisation functions as a result of conducting a Service Impact Analysis.

The time frame against each function represents the tolerance of the organisation to the loss of that function in isolation. The individual strategy for recovering each function should be guided by this time frame.

The recovery of each of these organisation functions must also conform to the fundamental recovery objective of re-establishing production for the core products outlined in the recovery strategy at the front of the plan.

Business functions are divided into 4 categories

- Category A functions – operational within 48 hours
- Category B functions – operational within one week
-

Directorates	Category A functions	Target Recovery Time
All Directorates	E- Mail / Internet	<48 hour
	Data services	<48 hours
	VPN Access Management	<48 hours
	Communications	
	Telecoms/ Reception	<48 hours

Department	Category B functions	Target Recovery Time
All Directorates	Databases / MIS and Operational	< 1 week
	Systems	
	Corporate Intranet	< 1 week
	Meetings	< 1 week
	Grants Management System (ICONI)	< 1 week

All remaining functions will be re-established after categories A, and B.

SERVICE RECOVERY	Tasks and Responsibilities

CMERT General Responsibilities

Establish communication links with nominated co-ordinators
Arrange regular meetings/briefings for department recovery progress reports.
Set out guidelines for department team leaders to prioritise Service Recovery needs.
Adjudicate on conflicting resource demands.
Ensure critical business activity has been identified.
Receive and approve activity schedules from the Departments (see Page 22)
Allocate appropriate office accommodation
Provide regular report to The Executive Office.
Monitor progress.

During this phase each service function will manage the recovery of their own functions as directed by the CMERT.

SERVICE RECOVERY	Department Activities

Director	Each one to be completed by Directorate
Directorate	

Overview of Service Functions				
Description of function	Maximum downtime	"Work around" method per each function – Contingency Plan	Alternative equipment required	Main IT applications used

VITAL RECORDS

Description Of Item	Location Within Work Area	Back Up Format	Back Up Location	Keys Etc.

EQUIPMENT Requirements (No.)

Machinery	PC	Printer	Telephone	Mobile	Photocopy.	Other
Day One						
Week One						
Week Two						

CRITICAL I.T. APPLICATIONS (Requirements)

APPLICATION	Day 1	Week	Month	Special Requirements

Recovery Milestones

The first two columns should be completed in advance of any incident. If disaster should strike, the tables can be used as checklists and the third column used to track recovery progress.

Day 1		
DESCRIPTION OF TASK	Responsibility	Done?
Hold team meeting at an agreed rendezvous. [This can be decided by staff at the time]	Director	
Identify priority functions to be undertaken by staff – categorise into: • Salvage and clearing materials at the affected site. • Establishment of core activities at the temporary relocation	Director	
Identify each function's critical service activity and concentrate efforts on these in short term.	Director	
Make schedules of critical work due to be produced and the due dates.	Director	
Progress report to the ERT	Director	

Day 2 – 3		
DESCRIPTION OF TASK	Responsibility	Done?
Agree where temporary activities can be conducted.	CEO	
Check layout of alternative accommodation and prepare timetable for occupation.	Director of Finance, Administration and Personnel	
Make arrangements for staff to attend alternate premises.	Director	
Advise the Switchboard at the alternate location of your telephone extension numbers.	Director	
Advise important contacts of your contact numbers at the alternate location.	Director	
Recover vital records.	Director	

Day 3 – 7		
DESCRIPTION OF TASK	Responsibility	Done?
Identify and record medium term activities for each member of staff.	Director	
Decide how to productively deploy less critical staff, pending return to full operation.	Director	
Confirm need to return to full strength and plan timetable for PC installation.	Director	
Review progress and all recovery milestones achieved.	Director	

All Phases	Contact Lists

Emergency Response Team Members

Title	Name	Work	Home	Mobile
The Chair	Peter Osborne			
Chief Executive Officer	Jacqueline Irwin			
Director of Finance, Administration and Personnel	Gerard McKeown			
Director of Cultural Diversity	Deirdre McBribe			
Director of Funding and Development	Paul Jordan			
Human Resources Manager	Jo Adamson			
Performance Management manager (ECNI)	Frank McWilliams			

Alternative Site Contact Details

Loss of Buildin g	NI Screen	Linda McGuiness	3rd Floor Alfred House, 21 Alfred Street, Belfast BT2 8ED	028 90268 591	LindaMc@northernirelandscreen.co.uk

Government Contact Details

Dept	Contact	Work Tel.
The Executive Office	Grainne Killen	02890523167
The Executive Office	Jamie Warnock	02890523167
The Executive Office	Kim Moylan	02890528270

Bank contact details

Bank	Contact person	Position	Work Tel	Fax/ E-mail
Bank of Ireland	Maria McAllister	Account Manager	02890433431	businessservicesteam@boi.com Maria. McAllister@BOI.com

Other Key External Contacts

Supplier	***Company***	***Name***	***Work Tel.***
Grant Management System	ICONI	Dean Carville	028 90 319 300
Communications Support	JComms	Chris Harrison	028 90 760 066
Files Archives	McConnell Archiving	Front Office	028 38 320 700
Telephone and Internet	Rainbow	Tim Balfour	028 9037 9000
HR Advice	Peninsula	Front Office	0844 892 2786
Solicitor	JCB Solicitors	Adam Brett	028 90 642 290
Internal Audit	ASM	Jonathan Buick	028 90 292 222
Payroll	Finegan Gibson	Margaret McMullan	028 90 325 822
Mobile phones	O2	Ian McKeown	028 90 960 366
Statutory Audit	NIAO	Kathy Doey	028 9025 1100
SAGE Support	Acorn	Carol McNicholl	028 7964 4975