Charnwood Borough Council

Information and Communication Technology (ICT) Resilience Strategy 2004

April 2004
# Table of Contents

1 INTRODUCTION ............................................................................................................................... 3
   1.1 PURPOSE AND SCOPE .................................................................................................................. 3
   1.2 BACKGROUND .............................................................................................................................. 3
   1.3 RELATIONSHIP WITH OTHER DOCUMENTS ............................................................................... 3
   1.4 MONITORING AND UPDATE ......................................................................................................... 4
   1.5 ASSUMPTIONS ............................................................................................................................... 4

2 MANAGEMENT SUMMARY .............................................................................................................. 5

3 MAIN PRINCIPLES .............................................................................................................................. 6
   3.1 AIMS ............................................................................................................................................... 6
   3.2 RESILIENT SERVICE PROVISION .............................................................................................. 6
   3.3 PRIORITISATION .......................................................................................................................... 6
   3.4 PARTNERSHIP .............................................................................................................................. 7
   3.5 FUNDING ....................................................................................................................................... 7

4 PREVENTATIVE MEASURES ............................................................................................................... 8
   4.1 REDUCING RISK ............................................................................................................................ 8
   4.2 ENVIRONMENT .............................................................................................................................. 8
   4.3 HIGH AVAILABILITY ..................................................................................................................... 9
   4.4 EQUIPMENT ................................................................................................................................... 9
   4.5 MAINTENANCE ............................................................................................................................. 9
   4.6 SPARES .......................................................................................................................................... 9
   4.7 BACKUP ....................................................................................................................................... 10
   4.8 SOFTWARE .................................................................................................................................. 10
   4.9 PROTECTION ................................................................................................................................ 10
   4.10 INSURANCE ................................................................................................................................. 10

5 RECOVERY ACTIONS ........................................................................................................................... 11
   5.1 RECOVERY ................................................................................................................................... 11
   5.2 INCIDENT MANAGEMENT .......................................................................................................... 11
   5.3 RESPONSIBILITIES ....................................................................................................................... 11
   5.4 PROCEDURES AND PRACTICES ................................................................................................. 11

6 BUSINESS CONTINUITY ACTIONS .................................................................................................. 12
   6.1 DISASTER RECOVERY .................................................................................................................. 12
   6.2 BUSINESS CONTINUITY MANAGEMENT ................................................................................... 12

7 GLOSSARY OF TERMS ....................................................................................................................... 13
1 Introduction

1.1 Purpose and scope

The purpose of this document is to detail key aspects of the Council’s ICT Resilience Strategy. It will be used as the basis for defining and funding how ICS deals with the risks associated with the infrastructure for which ICS has a responsibility.

The scope does not include actions required upon a major disaster e.g. the loss of the computer room through a terrorist attack etc. This will be covered under the Council’s Business Continuity Strategy.

This is not intended to be a detailed technical document because, too much detail would restrict its readership and a major review of Business Continuity is soon to take place.

1.2 Background

In March 2004 the Council issued its first Strategic Risk Register. One of the 30 Strategic Risks identified was the Failure of IT Systems (Risk 29).

This strategy deals with reducing the risk and the applicable risks identified on its risk assessment for Information Security Management, and the recovery methods deployed should an incident occur.

This strategy should be read in conjunction with: -

- The ICT Strategy
- The Council’s Strategic Risk Register
- The ISMS Risk Register
- The IT Security Policy
- The Council’s Business Continuity Strategy (not yet produced)

The objective of the ICT service is to help the organisation to achieve its goals, through a well-managed Council. The ICT Resilience Strategy is designed to help reduce the risks involved on the dependency of ICT thus assisting in this objective.

1.3 Relationship with other documents

A number of ICT related policies and procedures are also in existence or being developed. These include: -

- ICT procurement
- ICT disposals
- IT Security
- Business Continuity.
- Virus protection and Control
- System Administration
These are regularly reviewed and updated.

1.4 Monitoring and update

The ICT Resilience Strategy document will be revised annually. Urgent changes may be made if necessary in order to support major decisions taken by the Council at any other time.

1.5 Assumptions

The following assumptions have been made:

a) The Council remains committed to the ICT funding identified in the Capital Programme.

b) The Council will continue to provide similar services.

c) The Council's locations from May 2004 will comprise:

- The main offices at Southfields
- The depot at Limehurst Avenue and when in operation Granite Way, Mountsorrel
- Lifeline, Victoria Street
- MaCaulay House
- Town Hall
- Sheltered units
- South Charnwood Leisure Centre
- Soar Valley Leisure Centre

d) The Council is to review its Business Continuity Strategy and identify any critical services required of ICS.
2 Management Summary

The Council has committed itself to significant and ongoing development of its ICT Services, with the needs of the citizen as the main consideration.

This document provides a framework for reducing the risk to those assets to keep the number of failures to a minimum and at the same time ensure that if a failure does occur, recovery is carried out in a speedy and efficient manner.

Not every disaster scenario can be foreseen or indeed every recovery method detailed but by good use of a standard set of procedures it should be possible to reduce the recovery time from such a situation to limit the negative effect on the business.

Section 3: The main principles behind the ICT Resilience Strategy.

Section 4: Preventative Measures.

Section 5: Recovery Actions.

Section 6: Business Continuity Actions.

Section 7: Glossary
3 Main principles

3.1 Aims
To achieve our aims we will:

- Ensure that a risk assessment of the IT systems and infrastructure is carried out annually and the results logged in the IT Risk Register.
- Ensure that all risks identified that could lead to the loss or failure of an IT system are reduced to the minimum level possible within the financial constraints of the Council.
- Work closely with any designated officers in respect of Business Continuity Management.
- Be active members of any future proposed Council incident response team
- Encourage users to be aware of the risks that are involved and the measures they can take to reduce those risks at the desktop.
- Explore how technology can be used to reduce identified risks.
- Ensure adequate infrastructure is in place to support effective systems and communications.
- Work with the County, City, other districts and agencies to explore ways of improving resilience and possible partnership working to aid recovery.
- Ensure that recovery plans are maintained and tested on at least an annual basis.

3.2 Resilient service provision
In harmony with the Council’s aim to achieve an excellent rating in the Comprehensive Performance Assessment, the aim of ICS will be to deliver significant improvements in the resilience of its IT infrastructure.

It is recognised that the ability of the organisation to introduce spare capacity is limited but wherever this is considered critical then it should be introduced. If this is not possible then alternative methods should be considered, e.g. Re-locatable recovery or Mobile recovery. When introducing new systems Business Services need to consider effective methods of recovery should a loss of the system occur.

3.3 Prioritisation
Should there be a major incident where more than one of the Council’s systems are out of action, the priority for the recovery of these systems will be given by any future proposed Council Incident Response team.

During this financial year the following projects are planned to increase resilience:

- Centralised backup with recovery from disc
- New Internet Service Provider with the addition of an alternative resilient line
- Email Server Clustering
3.4 **Partnership**

Private Sector partners will be appointed where they are able to provide skills and resources more efficiently than could be made available in-house, or where this would lessen the risk to the Council’s services.

3.5 **Funding**

New ICS projects have included Capital and Revenue funding for resilience to be included, as part of this year’s Financial Strategy, and this will be reviewed during the normal budget planning process. However, the majority of Systems that are already in place do not have alternative recovery in place and this will need to be reviewed in the Council’s Business Continuity Strategy along with the finances that will be required.
4 Preventative Measures

4.1 Reducing Risk
The Council faces a variety of risks each and every day. Such risks could, unless recognised and properly managed, cause unexpected and potentially catastrophic disruption to the business. Such risks include:-

- Damage or denial of access to business premises,
- Loss of critical services,
- Failure of critical suppliers,
- Fraud, sabotage and commercial espionage,
- Deliberate introduction of computer viruses,
- Loss of critical computer and other support systems,
- Loss of key staff.

Where disruption affects critical business processes the consequences can be severe and may include substantial financial loss, legal exposure due to an inability to deliver committed levels of service and a loss in credibility and confidence as the organisation is seen not to have managed the risk properly. The consequential damage can have much wider impact on the council’s reputation. Business Continuity Management (BCM) enables the council to identify and subsequently manage risks, ensuring that predetermined levels of operation can be maintained.

The Council’s strategy to preserve the availability of the council’s systems and infrastructure is to reduce the risk to its systems wherever possible and thus to keep the number of incidents to a minimum.

4.2 Environment
A high standard for the environment of all servers will be maintained. This is a purpose built room and consists of:

- Full air conditioning with temperature and humidity controls. There is a minimum of 2 units such that if one unit fails the other unit is still operating.
- A temperature control is installed to raise the alarm should the temperature exceed 27 deg C and thus give the opportunity to preserve the servers.
- An Uninterruptible Power Supply is installed to continue to provide power for a given period should there be a loss in the mains power.
- Physical access to the room is limited to only those who have authority to access the servers.
- A fire prevention system is installed to preserve the equipment, where possible, should a fire occur within the building.
- Cables are routed under floor to protect them from damage.
- A flood warning system is installed to indicate any water in critical areas of the computer room.
- Intruder alarms are fitted to the room.
• No food or drink is permitted in the room to prevent contamination of the servers. To reduce the build up of dust the room is regularly cleaned by specialist cleaners.

4.3 **High Availability**
Where ever possible use is made of a failover System to provide high availability. This has been done at present with:-

- Firewall
- Citrix Servers
- Email Server

And it is to be introduced this financial year with

- Centralised backup on the backup servers and tape libraries
- Internet connection

Monitoring of the failover should always be maintained to be aware that a failover may have occurred and hence no redundancy is then available.

The network infrastructure also has inbuilt resilience between each of the buildings with an alternative route being provided. The network is currently under review to improve the speed of failover from one unit to the other.

4.4 **Equipment**
Equipment is purchased from a reputable supplier and wherever possible from the same supplier to a set Standard. This gives a better understanding within the technical staff, as knowledge is not required of a large range of equipment types. Also when spare parts are kept then there is also not a need for a wide range. At present the preferred supplier for Servers is either SUN or Dell depending on the operating system and Stone for the desktops.

Servers are of a high specification and include redundant power supplies and have their disks in a raid array to limit the impact of failure. The administrator team monitor the performance of servers to ensure that memory, disc space is correct and servers are not reaching their capacity.

4.5 **Maintenance**
All equipment when purchased has a maintenance contract for a period of 3 years. In the case of Servers this should be a gold contract with a maximum of 8hr call out time. When units are reaching the end of their contract period a renewal should be taken out if the equipment is still in business use.

4.6 **Spares**
Where costs can be justified spares should be maintained for resilience of equipment. At present spares are held for the main network components and when
an item is replaced for business reasons any components that can be reused elsewhere are removed as spares.

4.7 **Backup**

To enable a swift recovery from either a virus attack or a malicious corruption of data, backups of all server data will be made on tape and taken on a daily basis in accordance with the IT Backup procedure. These backups will be stored either in data safes on site or with a third party supplier in a data safe offsite. At present our offsite facility is maintained with Iron Mountain in Dudley.

With the introduction of centralised backup a copy of data will be taken to disk and the ability to take snapshots of some of the critical databases will enable recovery to a shorter time frame. Where there are critical applications on desktops users are advised that they should seek to use the services provided by ICS to either backup or ghost a copy of their application/system.

4.8 **Software**

All master software of the council should be held by ICS in a data safe to ensure the speedy recovery of systems when required.

4.9 **Protection**

Protection of the council’s Information is also maintained by the use of antivirus software on all servers and desktops, the use of content checkers and firewall. These products should remain in use at all times and not be turned off by the users. At the present time McAfee is used as the antivirus product and Mailsweeper as the content checker. These products are to be reviewed. At present there is no vulnerability software in use by the council, we are reliant on notifications from manufacturers. A patching tool, Update Expert however is in use to keep servers and desktops up to date with patch releases. It is a requirement to assess the need for a vulnerability scanner in the next year.

To prevent malicious code being downloaded restrictions are placed on the firewall.

4.10 **Insurance**

An inventory of the council hardware is made available to the insurance section so that adequate insurance is maintained. If a server is lost then it is probably through insurance that a replacement will be obtained. At present the purchase lead-time for a Dell server is 7 to 10 days and for a SUN server approximately 14 days.
5 Recovery Actions

5.1 Recovery
It is critical to the council’s ongoing success that in the event of an incident or a disaster, that these occurrences are managed to ensure continuance of service and a speedy recovery to normal operations. An incident occurs once a service has an unplanned failure and continues until normal operations have been restored and the incident is declared as ended.

5.2 Incident management
Once an incident has been declared then a log of the incident is started. The problem is identified and any dangers removed immediately, including possible connections to the cause of the problem. Knowledge of the incident and its status is maintained at all times. Those that need to know are informed thoroughly on the status of the incident at all times.

All expenditure is recorded and carried out in accordance with financial regulations. A review of each incident will take place no later than a month following the closure of the incident to ensure any new procedures or practises, and or risk prevention actions are put into place.

5.3 Responsibilities
The incident team will be managed by the ICS Security Officer or in his absence the Communication Infrastructure Manager

The responsibility for recovery procedures will be the officer responsible for the system or application.

The ICS Security officer is responsible for maintaining the incident logs and for identifying any procedures or desk instructions that are required for future use.
The helpdesk is responsible for checking and updating all emergency contact lists on at least a monthly basis.

5.4 Procedures and Practices
Procedures and desk instructions are in place for those anticipated failures especially where the recovery process is a complex set of actions. Where the assistance of third party suppliers is required for recovery contact details must be maintained. A copy of all contact lists, strategies, policies and procedures must be kept in a fireproof safe and offsite.
6 Business Continuity Actions

6.1 Disaster Recovery

The Council must be able to recover from disasters within an acceptable timescale. Business Continuity Plans are being compiled at present and the first review of this Strategy should ensue that these timescales and expectations are implemented.

6.2 Business Continuity Management

ICS will take an active part in the business continuity management forum to ensure that it assists the business in the technology aspects of its continuity strategy and plans. The ICS Security Officer will be the ICS representative for business continuity issues.
7 Glossary of Terms

*High Availability*
The ability to provide end users with access to a service for a high percentage of time while reducing unscheduled outages

*Legacy systems*
These are applications that were developed in the past, and are not able to support electronic service delivery.

*Mobile Recovery*
This caters for situations where computing facilities are rendered inoperable, and the disaster also affects the premises or access to the premises is not possible due to an incident in the locality.
A Mobile computer machine room complete with contracted back up system is despatched to designated site.

*Re-locatable Recovery*
A rapid 'ship-to-site' service designed to remedy a technical failure or theft. A replacement system and/or equipment is delivered and installed to site.