

Business Continuity Policy



Scottish Information
Commissioner

Contents

Glossary and abbreviations	i
Introduction	2
Policy	2
Roles and Responsibilities	2
Time.....	2
Location	3
Quality Assurance	3
Business Continuity Exercises	3
Audit	3
Document control sheet	4

Glossary and abbreviations

Term used	Explanation
SIC	Scottish Information Commissioner
SMT	Senior Management Team
BCP	Business Continuity Plan
HOCS	Head of Corporate Services

Introduction

1. This Business Continuity Policy defines the SIC's approach to maintaining continuity for the conduct of its business.
2. The maintenance of effective business continuity arrangements is an element of good corporate governance and the responsibility of senior management.
3. It is not possible for an organisation to anticipate every potential incident. However SIC's Business Continuity Plan (BCP) provides the capability for an effective response should a serious incident occur. Serious incidents include fires, floods, power cuts, epidemics and pandemic.
4. The BCP increases the resilience of the organisation by maintaining a capability for responding to unexpected incidents, minimising the extent of financial and reputational damage by having a comprehensive recovery plan to be implemented within a pre-determined timescale.

Policy

5. The SIC will maintain a Business Continuity Plan which supports the achievement of recovery within the following key parameters:

Roles and Responsibilities

6. The SMT has overall responsibility for ensuring the BCP is comprehensive and effective.
7. The Initial Response Team (SMT) is responsible for determining the extent of the disaster and for deciding to implement the BCP.
8. The HOCS has lead responsibility for BCP implementation
9. The Core Recovery Team, comprising key staff from each functional team as detailed in the BCP, has responsibility for implementing the recovery plan.
10. All staff are expected to work flexibly and responsively during periods that require deployment of the BCP.

Time¹

11. Following an incident which renders the SIC's office and IT systems wholly or partially unusable:
 - (i) Day 1: The Initial Response Team will meet to assess the extent of the disaster and, if appropriate, take the decision to implement the BCP including implementation of a communications plan
 - (ii) Day 2: The Core Recovery Team, comprising key staff from each functional team, will implement the BCP and, if necessary, relocate at the alternative location detailed in the BCP
 - (iii) By Day 5: Full recovery of IT systems will have been achieved

¹ Timescales are counted in business days

- (iv) By Day 6: Full service will resume, with staff operating from the alternative location, if necessary.

Location

- 12. Incidents can vary in their severity and impact. The BCP identifies an initial alternative operating location which may be used by some or all staff, depending on the prevailing circumstances.
- 13. Thereafter, the SMT may arrange medium term accommodation pending restoration of the Commissioner's office, if appropriate.

Quality Assurance

Business Continuity Exercises

- 14. Comprehensive testing of elements of the Business Continuity Plan will be carried out periodically.

Audit

- 15. An audit of BCP will be undertaken by Internal Audit periodically.

Scottish Information Commissioner

Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610

f 01334 464611

enquiries@itspublicknowledge.info

www.itspublicknowledge.info

© Scottish Information Commissioner 2017

You may use and re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence v3.0. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>