Business Continuity Policy

Scottish Information Commissioner

Contents

Glossary and abbreviations

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

Please note:

As a result of the impact of the COVID-19 pandemic, the following actions have been taken:

- **the office premises have been closed temporarily since 23 March 2020 and remain closed**
- **the DPO and other external parties have been informed of the temporary closure of the office premises and are updated following each SMT review of this decision**
- **office security and IT security measures are in place whilst the office premises are temporarily closed**
- **all members of staff are working remotely (with remote access to the office systems) using laptops and mobile phones provided by us and this includes the Commissioner and all members of the SMT**

- **updated guidance has been issued to staff working remotely covering:**
    - **security of information, including data protection**
    - **records management - staff working remotely must comply with our information and records management procedures including ensuring that our records are trustworthy, complete, accessible, legally admissible in court and robust**
    - **data incident procedures**
    - **how to use Microsoft Teams and guidance on use**

This Business Continuity Policy and the related Business Continuity Plan are currently under review.

If you have any questions about the operation of this Business Continuity Policy please contact the HOCS (Helen Gardner-Swift) or the FAM (Liz Brown).

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.

Time[1]

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.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status. *E.g. C5 Key Documents Handbook v01 CURRENT ISSUE*	C5 Business Continuity Policy v01 CURRENT ISSUE
VC FileId	85362
Type	Policy
Approver	SMT
Responsible Manager	HOCS
Date of next planned review	March 2022
Approval & Publication	
Approval Date (major version)	13/03/17
For publication *(Y/N)*	Yes
Date published	11/06/21
Name of document in website file library	BusinessContinuityPolicy
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	07/06/21

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36**)***	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOCS, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
20/03/17	KB	01.01	01.02	DCS updated, published on website
07/06/21	HGS	01.02	01.04	Updated HOOM reference to HOCS, added in paragraph re: COVID -19 pandemic and review of policy and updated DCS
11/06/21	BOW	01.04	01.05	DCS updated, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info