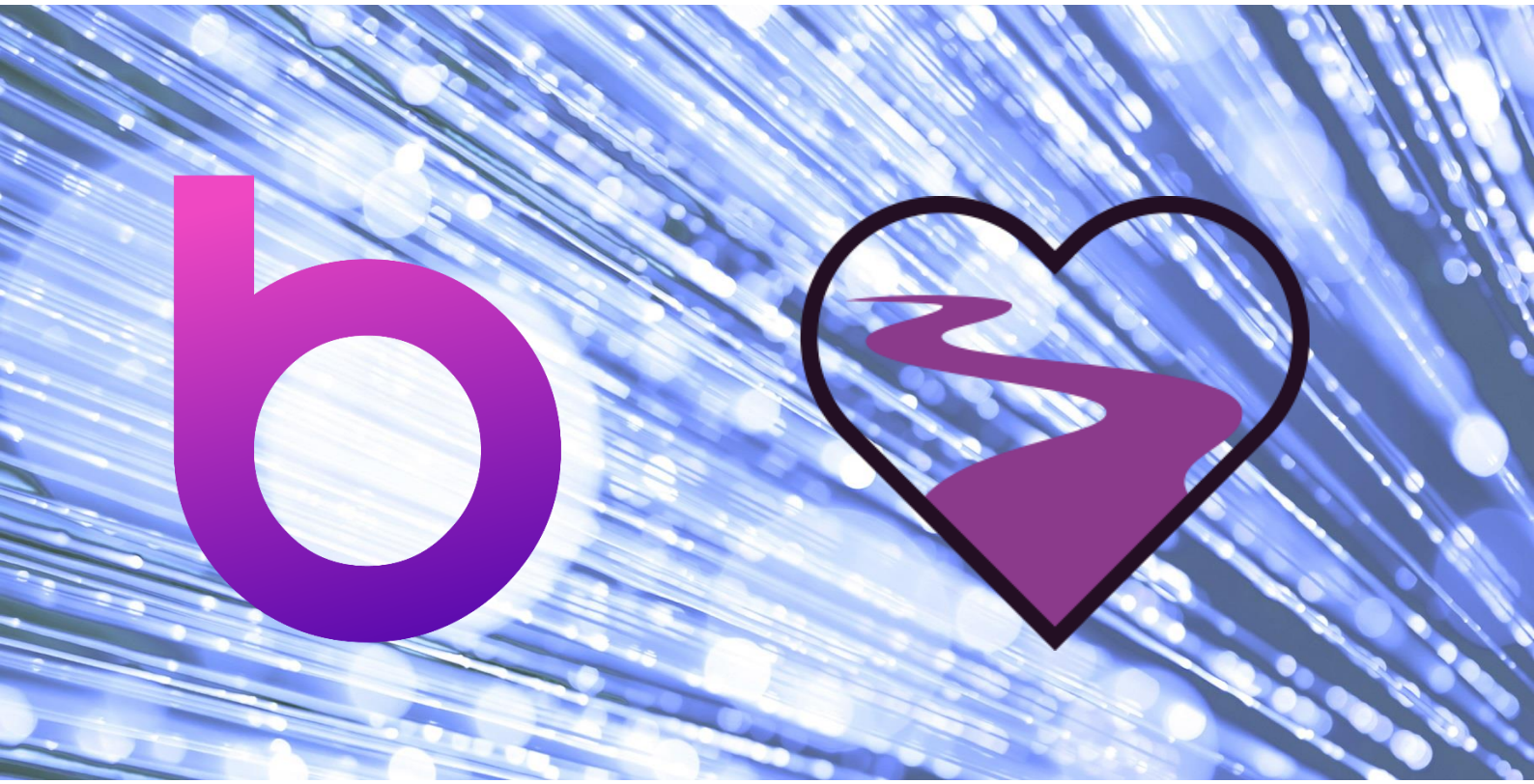
Business Continuity

Upstream Outcomes Policy

(Supporting Bridgit Care & Upstream health Business Units)

Author: D Crombie
Date: 04/04/2022
Version: 2.0



Information and technology
for better health and care

Contents

1 Background

This policy is based on NHS Digitals example policy and aligns to the recommendations and approach adopted by NHS Digital. This is based on the NHS Digital template dated 23rd May 2017.

2 Approval / update history

Version ID	Description	SIRO Approval
1.0	Initial version for release	08/10/2018 : Darren Crombie
2.0	Updated version following 2022 review	05/04/2022 : Darren Crombie

Terminology

Term	Definition
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

Policy

*The Business Continuity Policy **shall** be used to enable Upstream Outcomes to produce, implement, test and manage a Business Continuity Plan (management system) on Upstream Outcomes IT systems to enable a structured recovery post an IT or information security incident. This policy relates to the IT and information elements of the overall Upstream Outcomes approach to Business Continuity.*

Business Continuity Definition

- *Business Continuity is defined as the capability of Upstream Outcomes to continue delivery of products or services at acceptable predefined levels following a disruptive incident.*

Business Continuity Approach

- *Upstream Outcomes **shall** use the "Plan-Do-Check-Act" (PDCA) model to plan, establish, implement, operate, monitor, review, maintain and continually improve the effectiveness of its Business Continuity Plan for IT and information.*

Business Continuity Plan

- *A Business Continuity Plan **shall** be produced to enable immediate responses to be made to an information security incident (IT or information).*
- *The Plan **shall** be regularly tested, it is suggested that this is at least annually.*
- *The Plan **should** cover:*
  - *Ownership – which post owns and controls the plan*
  - *Responsibilities – identification of roles and their responsibilities*
  - *Scope – what is in the plan and what is out of the plan*
  - *Identification of critical assets with priority order for recovery/business functionality*
  - *Capabilities – identified internal and external capabilities*
  - *Resources – allocation of tasks to resources, internal and external*
  - *Communication process*
  - *Task flow – including:*
    - *Points of contact*

- *Relationship to incident management team*
- *Response actions*
- *Recovery/restoration of asset or standing up of identified alternate*
- *Recording of actions taken and time when assets recovered/restored.*

- *Post Action Review – lessons learnt.*
- *Test Schedule.*

Responsibilities

- *The following roles **shall** undertake the responsibilities listed:*
  - *Senior Information Risk Owner (SIRO) – coordinate the development and maintenance of the Business Continuity Plan – ensuring it relates to the overall Upstream Outcomes Business Continuity Strategy.*
  - *Business Continuity Plan Manager – maintains the Plan on behalf of the SIRO ensuring that testing is undertaken. A post **shall** be allocated for this role.*
  - *Information Asset Owners (IAOs) – ensure that the requirements from the Business Continuity planning are adequately considered and documented for all information assets of which they have ownership; and, enable the recovery to be enacted.*
  - *Line Managers - ensure that staff follow the Upstream Outcomes Business Continuity Plan procedures.*
  - *Chief Information Security Officer (CISO) – management of business continuity procedures relating to IT and information security.*

Given the scale of Upstream Health currently all of these roles fall under the responsibility of the Chief Executive Officer (CEO).

Training and Awareness

- *Personnel who are required to undertake specific technical and functional roles associated with business continuity **shall** be trained and formally qualified to complete this specialist function.*
- *All Upstream Outcomes staff, including third parties, **shall** be made aware of the requirements of the Upstream Outcomes Business Continuity Plan and subsequent Procedures.*

Management and Implementation

- *The Business Continuity Policy and the resulting Business Continuity Plan **shall** be reviewed and re-issued annually or upon identification of a change in procedure or lesson learnt.*
- *The effectiveness of the Policy and Plan **shall** be monitored through audits and tests (external and internal) and from lessons learnt during any business continuity activity.*

Testing

- *On behalf of the SIRO the Business Continuity Plan Manager **shall** coordinate and manage testing which **should** follow the below levels and is recommended to be at least annually at each level:*

- *Table Top*
- *Walkthrough*
- *Real-time Live Test*

3 Key Words

Business Continuity, CISO, Data Recovery, IAO, SIRO,