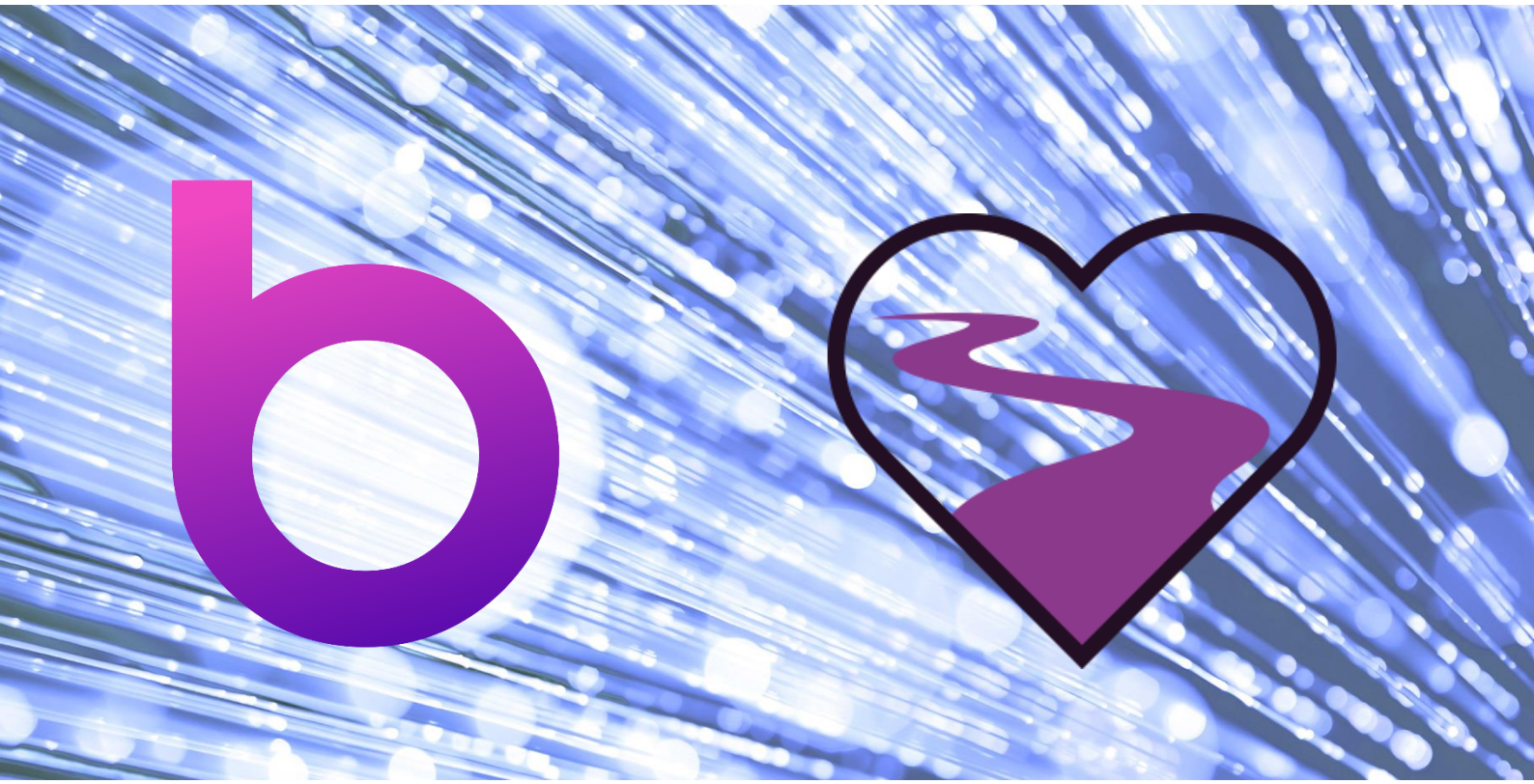
Patching

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	Meaning/Application
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

[Patch management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organisation. Best practice is to deploy security updates and patches in a scheduled and predictable manner. Scheduled security updates and patches would be excluded if it can be proved that this security update causes problems for the system, software, etc. The security update would then be re-scheduled for next release.]

IT Infrastructure and associated components

- *Upstream Outcomes **shall** comply with the minimum baseline requirements that are contained in this policy. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Upstream Outcomes assets and the data that resides on the system.*
- *Any exception to this policy **shall** be documented and forwarded to Upstream Outcomes Management for review and endorsement or rejection.*

Applications

- *Any applications (both commercial-off-the-shelf (COTS) and in-house) owned or managed by Upstream Outcomes **shall** be updated with the necessary security patches. This is the default configuration for all applications.*
- *Any exception to this policy **shall** be documented and forwarded to Upstream Outcomes Management for review and endorsement or rejection.*

Roles and Responsibilities

- *Upstream Outcomes IT Service Operations and Systems Management **shall** manage the patching needs for:*
    - *All IT infrastructures on the network and associated components owned or managed by Upstream Outcomes.*
    - *All applications ((COTS or in-house) owned or managed by Upstream Outcomes.*
- *Upstream Outcomes Security **shall** be responsible for routinely assessing compliance with the patching policy and will provide guidance on issues of security and patch management.*

- *The Change Management Board **shall** be responsible for approving the monthly and emergency patch management deployment requests – in line with the Upstream Outcomes Change Approval Board (CAB) process.*

Monitoring and Reporting

- *Upstream Outcomes IT Service Operations and Systems Management <or equivalent department> **shall** compile and maintain reporting metrics that summarize the outcome of each patching cycle.*
- *Upstream Outcomes Management **shall** use these reports to evaluate the current patching levels of all systems and to assess the current level of risk.*
- *These reports **shall** be made available to Upstream Outcomes Security and Internal Audit <or equivalent departments> upon request.*

Enforcement

- *Upstream Outcomes Security and Internal Audit **shall** <or equivalent departments>, without notice, conduct random assessments to ensure compliance with the principles of this policy.*
- *Any system found in violation of this policy **shall** require immediate corrective action.*

Exceptions

- *Exceptions to the Upstream Outcomes Patching policy **shall** require formal documented approval from Upstream Outcomes Security <or equivalent department>.*
- *Any servers, workstations or applications that do not comply with this policy **shall** have an approved exception on file with Upstream Outcomes Security <or equivalent department>.*

3 Key Words

Applications, Audit, Change, Data, Hotfix, Information, Infrastructure, Patch, Service Pack