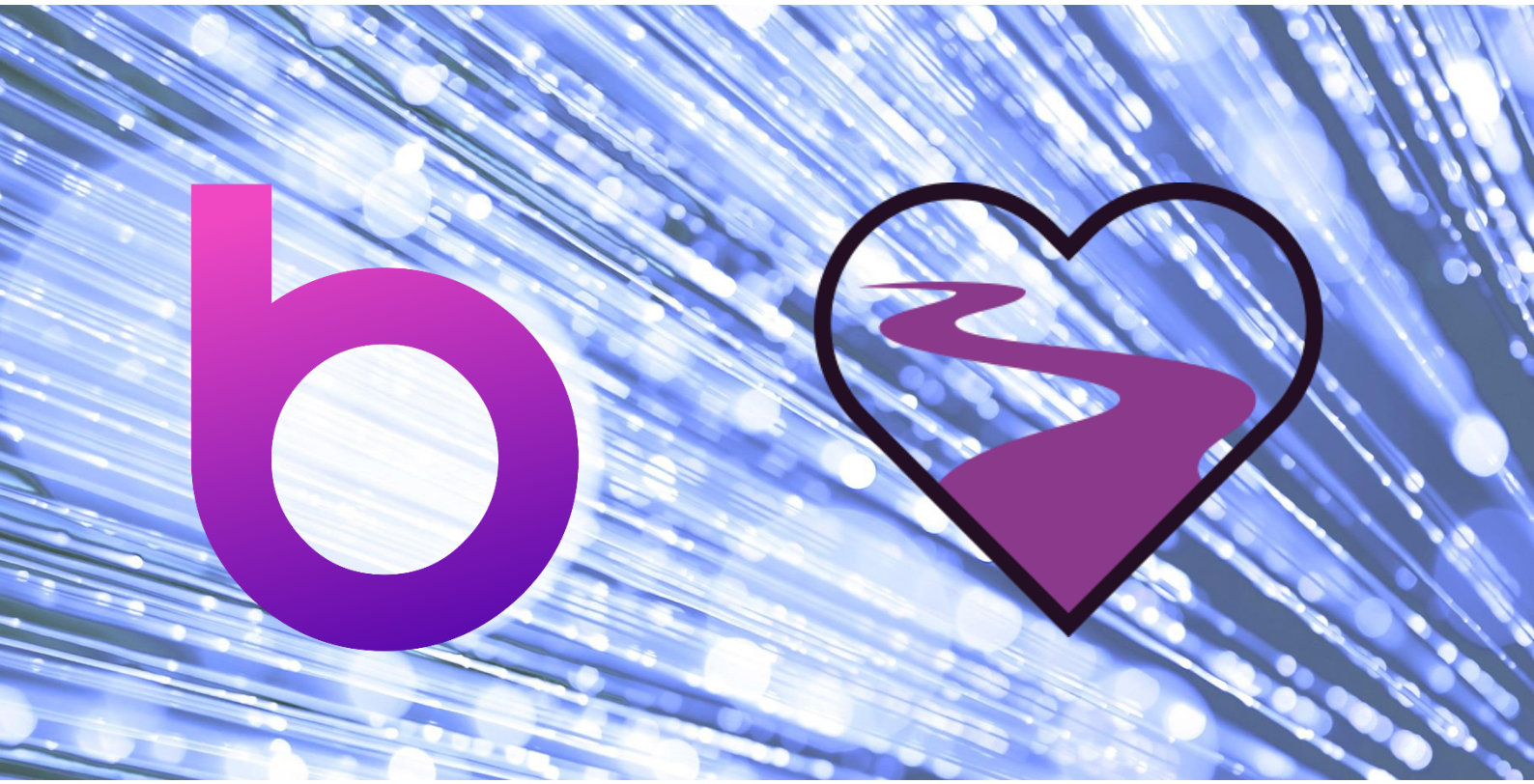
Anti-Virus and Malware

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 3
2 Approval / update history 3
Terminology 4
Policy 4
General 4
Administrative 4
3 Key Words 5

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

General

- *Upstream Outcomes systems **shall** run effective anti-virus and anti-malware software.*
- *Upstream Outcomes IT anti-virus and anti-malware software **shall** be configured to detect and remove known viruses and malware.*
- *All Upstream Outcomes IT systems (servers, desktops, laptops) **shall** run one of the NHS approved and supported anti-virus and anti-malware software packages.*
- *All servers, desktops and laptops **shall** be configured to run only one of the approved products at any time.*
- *Anti-virus and anti-malware software **shall** be kept up to date.*
- *Anti-virus and anti-malware definition files **shall** be kept up to date.*
- *Anti-virus and anti-malware software updates **shall** be deployed across the network automatically following their receipt from the vendor.*
- *Virus and malware signature updates **shall** be deployed across the network automatically following their receipt from the vendor.*
- *Anti-virus and anti-malware software **shall** be configured for real time scanning and regular scheduled scans.*
- *Tamper protection **shall** be enabled to prevent end users or malware altering the anti-virus and anti-malware software's configuration or disabling the protection.*
- *All IT equipment and removable media **shall** be scanned for viruses and malware before being introduced to the Upstream Outcomes network, system or device.*
- *IT systems infected with a virus and malware that the anti-virus or anti-malware software has not been able to deal with **shall** be quarantined from the NHS network until virus free.*
- *Any instance of virus or malware infection or detection **shall** be documented and raised as a security incident.*

Administrative

- *Changes that are required to the settings of any of anti-virus or anti-malware products **shall** follow the formal Upstream Outcomes change control process.*

- *Upstream Outcomes **shall** ensure that all anti-virus and anti-malware products are regularly and correctly updated from the vendor service.*
- *Upstream Outcomes **may** periodically test anti-virus and anti-malware defences by deploying a safe and non-malicious test file.*
- *A log **shall** be kept of all scans undertaken, these logs **should** record as a minimum:*
  - *Date.*
  - *Time.*
  - *Addresses of areas scanned.*
  - *Malware found.*
  - *Any action taken by the anti-virus and anti-malware software (e.g. quarantine or delete).*
- *To prevent misuse and tampering by unauthorised staff, all administrative settings in the deployed anti-virus and anti-malware products **shall** be secured by means of a password.*

3 Key Words

Malware, Virus, Software, Systems.