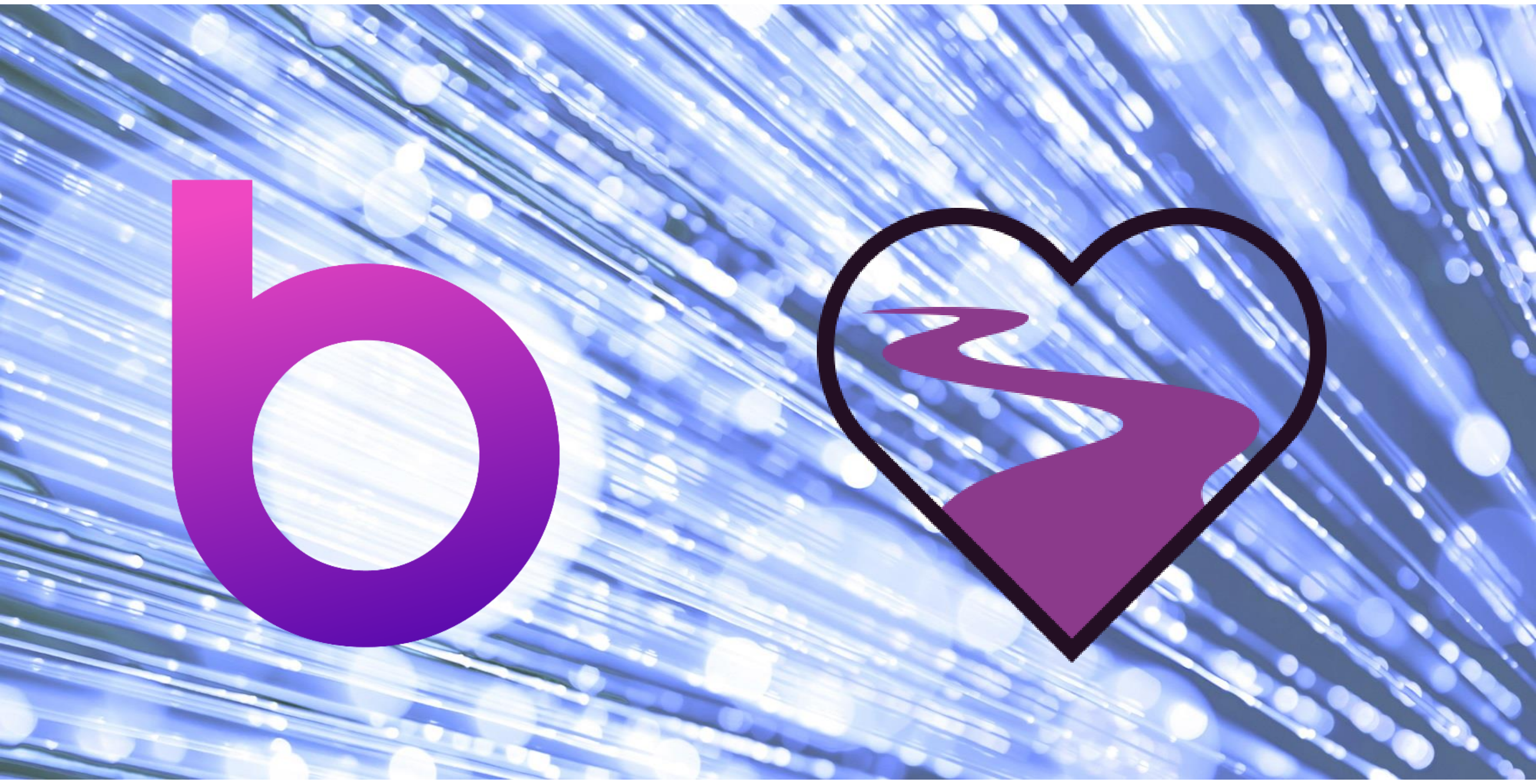
Information Security

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

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of Upstream Outcomes information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies. It supports the 7 Caldicott principles and 10 data security standards. This policy covers:

- *Information Security Principles.*
- *Governance – outlining the roles and responsibilities.*
- *Supporting specific information security policies – Technical Security, Operational Security and Security Management.*
- *Compliance Requirements.*

Information Security Principles

The core information security principles are to protect the following information/data asset properties:

- *Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.*
- *Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.*
- *Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.*

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

For the NHS, the core principles are impacted, and the effect aggregated, when any data breach relates to patient medical data.

Governance – Roles and Responsibilities

All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting Upstream Outcomes business. All staff are responsible for information security and remain accountable for *their actions in relation to NHS and other UK Government information and information systems. Staff **shall** ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.*

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within Upstream Outcomes and advises the Board on the effectiveness of information risk management across the organisation. Operational responsibility for Information Security within Upstream is also take by the SIRO due to the small scale of the organisation

*All Information Security risks **shall** be managed in accordance with the Upstream Outcomes Risk Management Policy.*

Chief Information Security Officer

*The Chief Information Security Officer is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The Information Security Officer **shall**:*

- *Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.*
- *Provide a central point of contact for information security.*
- *Ensure the operational effectiveness of security controls and processes.*
- *Monitor and co-ordinate the operation of the Information Security Management System.*
- *Be accountable to the SIRO and other bodies for Information Security across Upstream Outcomes.*
- *Monitor potential and actual security breaches with appropriate expert security resource.*

Within Upstream this is a secondary role for the Information Governance lead.

Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

This role is provided in Upstream by the Information Governance lead with the support of the Upstream Clinical Director.

Data Protection Officer

*The Data Protection Officer is responsible for ensuring that Upstream Outcomes and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer **shall**:*

- *Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.*

- *Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).*
- *Communicate and promote awareness of the Act across the Upstream Outcomes.*
- *Lead on matters concerning individuals right to access information held by Upstream Outcomes and the transparency agenda.*

Within Upstream this is a secondary role for the Information Governance lead.

Information Asset Owners

*The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and **shall** be responsible for:*

- *Understanding what information is held.*
- *Knowing what is added and what is removed.*
- *Understanding how information is moved.*
- *Knowing who has access and why.*

Within Upstream this is a secondary role for the Information Governance lead.

Senior Responsible Owners

*All Senior Managers, Heads of Department, Information Risk Owners and Directors, defined as Senior Responsible Owners (SROs), are individually responsible for ensuring that this policy and information security principles **shall** be implemented, managed and maintained in their business area. This includes:*

- *Appointment of Information Asset Owners (IAO) to be responsible for Information Assets in their area(s) of responsibility.*
- *Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks*
- *Supporting personal accountability of users within the business area(s) for Information Security*
- *Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.*

Within Upstream this is the responsibility of the Chief Executive Officer (CEO).

Supporting Policies

The Information Security Policy is developed as a pinnacle document which has further policies, standards and guides which enforce and support the policy. The supporting policies are grouped into 3 areas: Technical Security, Operational Security and Security Management and are shown in the diagram overleaf. The Information Security Policy is closely aligned to the NHS Information Governance Strategy and relies upon, and supports, the Upstream Outcomes Physical and Personnel Security policies.

Technical Security

The technical security policies detail and explain how information security is to be implemented. These policies cover the security methodologies and approaches for elements such as: network security, patching, protective monitoring, secure configuration and legacy IT hardware & software.

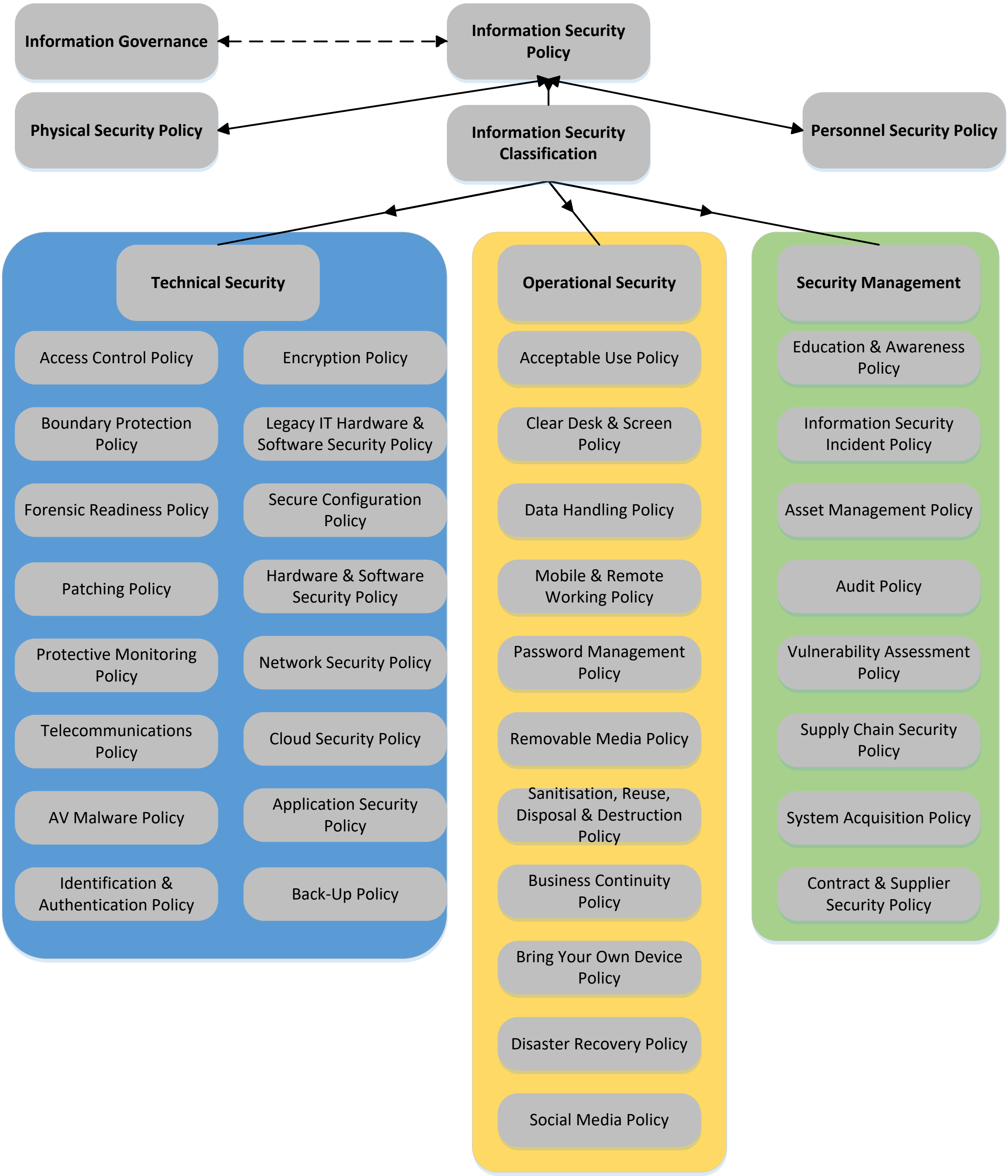
Operational Security

The operational security policies detail how the security requirements are to be achieved. These policies explain how security practices are to be achieved for matters such as: data handling, mobile & remote working, disaster recovery and use of social media.

Security Management

The security management practices detail how the security requirements are to be managed and checked. These policies describe how information security is to be managed and assured for processes such as: information security incident response, asset management and auditing.

At Upstream we have a single document for each of the key areas and then separate documents for specific areas where additional detail is needed.


Information Governance
Information Security Policy
Physical Security Policy
Information Security Classification
Personnel Security Policy
Technical Security
Access Control Policy
Encryption Policy
Boundary Protection Policy
Legacy IT Hardware & Software Security Policy
Forensic Readiness Policy
Secure Configuration Policy
Patching Policy
Hardware & Software Security Policy
Protective Monitoring Policy
Network Security Policy
Telecommunications Policy
Cloud Security Policy
AV Malware Policy
Application Security Policy
Identification & Authentication Policy
Back-Up Policy
Operational Security
Acceptable Use Policy
Clear Desk & Screen Policy
Data Handling Policy
Mobile & Remote Working Policy
Password Management Policy
Removable Media Policy
Sanitisation, Reuse, Disposal & Destruction Policy
Business Continuity Policy
Bring Your Own Device Policy
Disaster Recovery Policy
Social Media Policy
Security Management
Education & Awareness Policy
Information Security Incident Policy
Asset Management Policy
Audit Policy
Vulnerability Assessment Policy
Supply Chain Security Policy
System Acquisition Policy
Contract & Supplier Security Policy

Compliance Requirements

Legislation

*Upstream Outcomes is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation **shall** be devolved to employees and agents of Upstream Outcomes, who **may** be held personally* *accountable for any breaches of information security for which they **may** be held responsible. Upstream Outcomes **shall** comply with all relevant legislation appropriate; this includes but is not limited to:*

- *Data Protection Act 1998*
- *Freedom of Information Act 2000*
- *Health & Social Care (Safety & Quality) Act 2015*
- *Computer Misuse Act 1990*

Audit

*Audit will be performed as part of the ongoing Upstream Outcomes Audit Programme and the Information Security Officer **shall** ensure appropriate evidence and records are provided to support these activities at least on an annual basis.*

Within Upstream the Information Governance Lead will coordinate this.

Review

*This policy **shall** be reviewed at least annually by the reviewers noted within the Reviewers section of this policy. The Information Security Officer **shall** be responsible for ensuring the review is conducted in good order and follows due process for approval.*

The Information Security Officer is accountable for providing the results of ongoing reviews of information security implementation across Upstream Outcomes. This includes support to the annual Information Governance Toolkit return.

Within Upstream the Information Governance Lead will coordinate this.

3 Key Words

Information Security, Governance, Confidentiality, Integrity, Availability, Senior Information Risk Owner, Senior Risk Owner, Information Asset Owner, Information Security Officer, Data Protection Officer, Caldicott Guardian