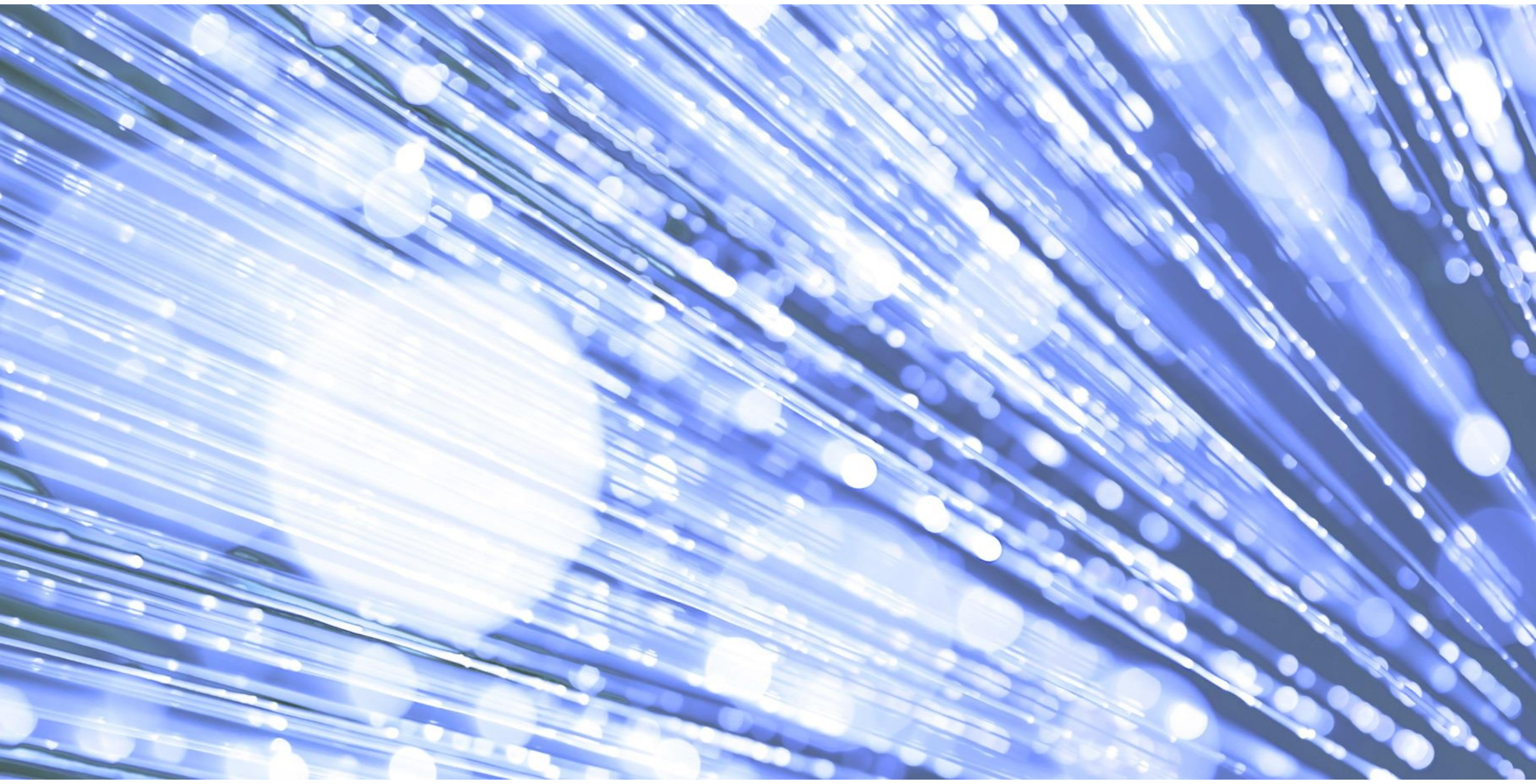
NHS Digital

Dr Chaudhury's Practice

Information SecurityPolicy Updated for GDPR 10.05.2018 review date 10.05.2019

0



Information and technology
for better health and care

Contents

1 Purpose

The purpose of this Information Security Example Policy is to provide exemplar guidance in line with HMG and private sector best practice for the production of an Information Security Policy appropriate for the organisation. This is in order to allow the reader to produce the necessary policy and guidance for their business area and to ensure that the applicable and relevant security controls are set in place in line with the Department for Health, the wider NHS, health and social care and HMG requirements.

2 Scope

The drafting of any policy governing the production of an Information Security policy for systems, devices or applications and information deployed in support of NHS or health and social care business functions.

3 Applicability

This Example Policy is applicable to and designed for use by any NHS, health and social care or associated organisations that use or have access to NHS systems and/or information at any level.

4 Guidance

This Example Policy provides guidance on the production of an Information Security Policy. The Example Policy is in italics with areas for insertion shown as <> and the rationale for each paragraph or section, where required, in [….].

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 <insert name of organisation> 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.*

[This section aims to outline why the policy is required and the main drivers for it.]

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.

[This section describes the main information properties and the additional issues of the impact on confidentiality of aggregated data, either by association or volume, and the requirement to consider reputational impacts.]

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 <insert name of organisation> 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

Dr P K Chaudhury

Mrs Ann Norman

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 <insert name of organisation>.*
- *Monitor potential and actual security breaches with appropriate expert security resource.*

[This paragraph is clearly applicable for larger organisations where there is a definitive team for security, including an information security officer. For smaller organisations, the principle of a named individual or role assuming responsibility for the provision of information security advice will need to be determined or the ability (and contact details) for that organisation to be able to call on the services of another organisation (potentially within the NHS or from an outsourced provider). For smaller organisations, this is likely to be a secondary role to their normal role within the organisation, often referred to as 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.

[The aim of the Caldicott Guardian is to ensure the organisation implements the Caldicott principles and data security standards; within larger organisations this is normally from a dedicated role. For smaller organisations, there is no need to appoint a Caldicott Guardian, but there is a need to have an Information Governance lead (sometimes referred to as a Caldicott lead) who, if they are not a clinician, will need support from a clinically qualified individual.]

Data Protection Officer

The Data Protection Officer is responsible for ensuring that <insert name of organisation> 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 <insert name of organisation>.*
- *Lead on matters concerning individuals right to access information held by <insert name of organisation> and the transparency agenda.*

[For larger organisations, such as NHS Trusts, there will be nominated, dedicated Data Protection Officers (DPOs); for smaller organisations, there are unlikely to be dedicated DPOs. However, the requirement remains for this role to be fulfilled; this could be the person or role nominated as 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.*

[The aim of the IAO role is to have a nominated role or person to be responsible for the management and control of information assets. Within larger organisations this is normally from a dedicated role. For smaller organisations, this role is likely to be undertaken by 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.*

[The aim of the SRO is to have nominated role(s) or person(s) for the implementation and management of IAOs and information security within the department or organisation. For larger organisations, this will be associated with senior managers and heads of departments. For smaller organisations, this role will be associated with one of the named partners or potentially the head of the organisation if it is a very small organisation.]

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 <insert name of organisation> 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.

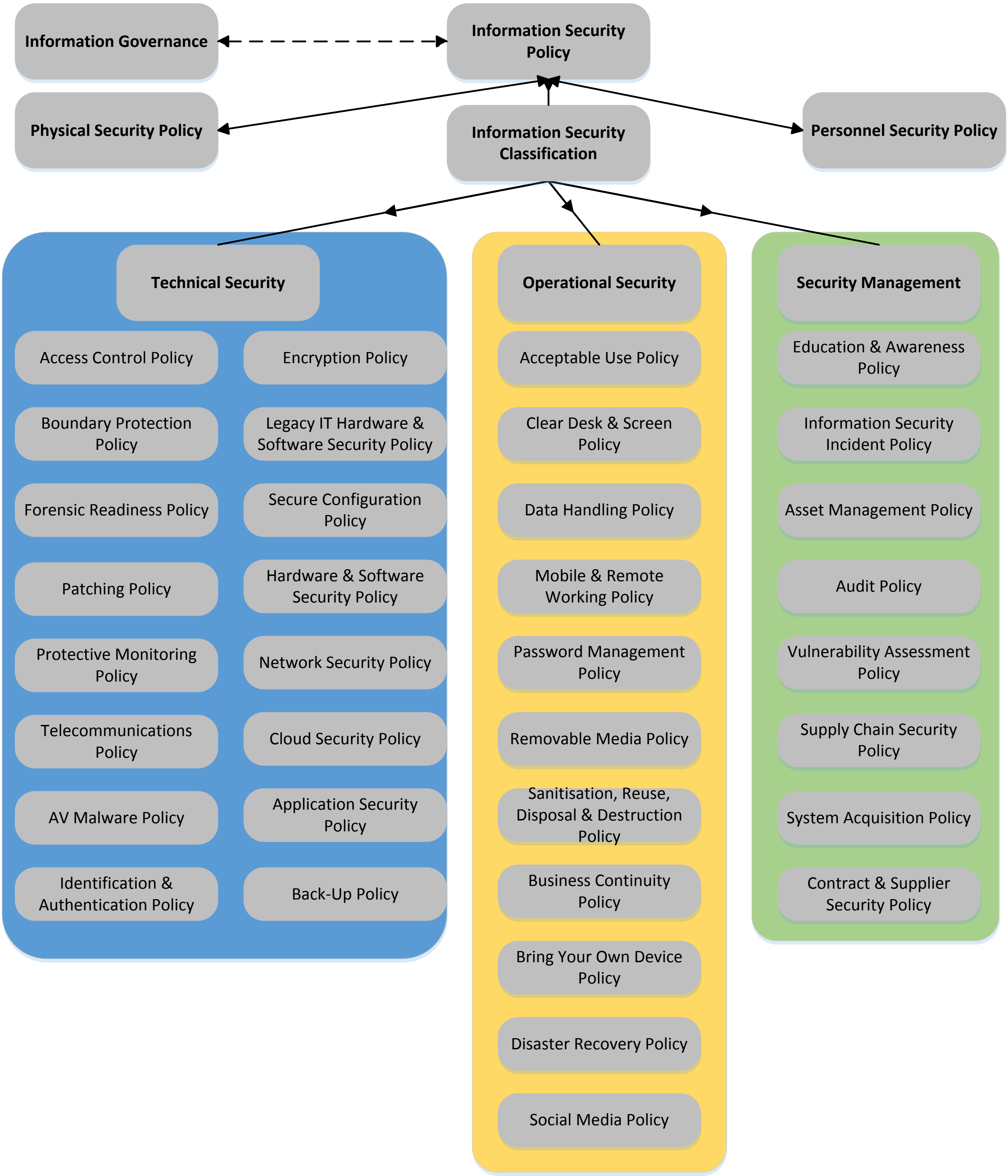
Operational Security

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.

[For larger organisations, the overleaf diagram on supporting policies will result in separate documents for each policy; however, for smaller organisations these may be combined or covered under a coverall for each area (technical, operational and security management). Some organisations will have outsourced their IT to a supplier or provider and therefore the information security policy and supporting policies will need to focus on the requirements and conditions to be implemented by the contacted provider.]


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

[The above diagram should be produced to reflect 'The Tree' or 'Framework' of policies that will be utilised by the organisation.]

Compliance Requirements

Legislation

<Insert name of organisation> 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 <insert name of organisation>, who* ***may*** *be held personally accountable for any breaches of information security for which they* ***may*** *be held responsible. <Insert name of organisation>* ***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*

[This section covers legislation that relates to information and IT systems management. The above acts are the minimum but if the organisation is subject to other legislation particularly relevant to IT or information management then these should be included.]

Audit

Audit will be performed as part of the ongoing <insert name of organisation> 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.*

[A regular auditing of the policy and the supporting policies is required. For larger organisations, this may be performed by a dedicated team and controlled by the Information Security Officer. For smaller organisations, the Information Governance Lead will coordinate this but the auditing may be completed by the outsourced IT provider and reported to the Information Governance Lead.]

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 <insert name of organisation>. This includes support to the annual Information Governance Toolkit return.

[Best practice and good management requires regular reviews of policies and a mechanism should be in place for reviews. For larger organisations, this will be coordinated by the Information Security Officer but for smaller organisations it will most likely be the Information Governance Lead who coordinates the reviews.]

5 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