Medicines & Healthcare products
Regulatory Agency

Information Security Policy

Accountable Director	John Quinn, Chief Technology Officer and SIRO
Date approved	26/02/2021
Review date	25/02/2023

Open Government Licence

Any enquiries regarding this publication should be sent to us at Medicines and Healthcare products Regulatory Agency.

Document Status

This is a controlled document. The controlled version is posted on the Agency intranet. You may print this document if you need to but be aware that it is only valid the day it is printed as the controlled version may change. For the same reason, do not save onto local or network drives.

Revision History

Version No.	Effective date	Author's Title	Change
1.0	12/04/2017	IT Security Officer	Incorporated minor comments from IAB members and expanded sections 4 and 5.
1.1	17/07/2018	IT Security Officer	Policy reviewed by IAB and PPC to ensure it is still fit for purpose.
1.2	05/03/2019	IT Security Officer	New clause added in respect of vetting of contractors.
2.0	26/02/2021	IT Security Officer	Update reflecting new guidance and technologies.

Consultation

Who	Date
John Quinn, CDIO and SIRO	March 2019
Information Security team and DPO	November 2020
Policy and Procedure Committee members	December 2020

Approval

Approval Path	Date
Avnesh Pandya, Deputy Director, TD[3]	26/02/2021
Policy and Procedure Committee	18/12/2020
Information Asset Board	21/01/2021

Replaces

Information Security Policy v.1.2

Contents

This table of contents contains hyperlinks. You can hover over a section and press ‘Ctrl’ and ‘click’ to go directly to it

1 Introduction

1.1 This document sets out the Agency's overarching Information Security Policy.

2 Scope

2.1 All the Agency's physical and information assets are within scope of this security policy.

2.2 Physical assets include, but are not limited to, premises, computer hardware, data cabling, telephone systems, filing systems and physical data files.

2.3 Information assets include, but are not limited to, data and information printed or written on paper, spoken in conversation or shown in films, or stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones as well as on CD ROMs, floppy disks, USB sticks, personal devices, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means.

2.4 'Data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, and utilities).

3 Policy

3.1 The Agency's Executive Committee (ExCo) and Unitary Board are committed to securing all the physical and information assets throughout the Agency to prevent unauthorised access, loss or damage. This is to preserve the confidentiality, integrity and availability of Agency information to safeguard public health, protect personal data, meet legal and contractual obligations and protect its commercial image and reputation.

3.2 The Agency's information security policy will be implemented through its Information Security Management System (ISMS). The ISMS is the set of policies and procedures for systematically managing the Agency's sensitive data.

3.3 The purpose of the Information Security Policy's is to define a framework so that the Agency's staff, service providers, and any external party using Agency information, are made aware of their responsibilities (defined in job descriptions or contracts) to:

- preserve information security
- report security breaches; and

- act in accordance with the requirements of the Information Security Management System (ISMS).

3.4 All Agency staff (and certain external parties identified in the ISMS) are expected to comply with this policy and ISMS. They will receive appropriate information security awareness training such as those mandatory training courses found on Civil Service Learning and other sessions the Information Security Team will run throughout the year.

3.5 The consequences of breaching the Information Security Policy are set out in the Agency's disciplinary policy; and in contracts and agreements with third parties.

4 Roles and responsibilities

4.1 The Senior Information Risk Owner (SIRO) is ultimately responsible for the management, maintenance and implementation of this security policy.

4.2 Legal and regulatory obligations and other roles and responsibilities in relation to the Information Security Policy are set out in the ISMS and the Information Governance Management Framework.

5 Procedure

5.1 The processes and standards that relate to the implementation of this security policy are set out in the Information Security Management System (ISMS).

5.2 The ISMS is a set of policies and procedures that are relevant to the security risks faced by the Agency. These procedures are for staff to implement in situations that present a security risk.

5.3 When applicable, the ISMS also sets out the standards that procedures need to meet to be effective in preventing a security breach and comply with this security policy.

6 Competence

6.1 Staff will receive appropriate training such as those mandatory training courses found on Civil Service Learning and other sessions the Information Security Team will run throughout the year to meet their responsibilities under the Information Security Policy. As a minimum, this will include mandatory security learning standards set out by Cabinet Office and Civil Service Learning.

6.2 In support of this Information Security Policy all service providers must ensure that all their staff, who in the course of their work have access to government assets (regardless of where located), are vetted to a minimum of the Baseline Personal Security Standard (BPSS).

6.3 Where is it is not possible or practical for a supplier to comply with this BPSS requirement, alternative equivalent methods will be considered on a case by case basis and addressed formally in writing.

7 Monitoring compliance

7.1 This security policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan within the ISMS and at least annually.

7.2 Monitoring compliance with this policy will be measured by the number and type of reported security incidents.

7.3 Security incident trends and lessons learnt will be reported to the Information Asset Board.

8 References

8.1 The following internal documents are associated with or linked to this document:

Internal Document	Document Location
Information Governance Management Framework	INsite | Policies and Procedures

8.2 The following external documents are associated with or linked to this document:

External Document	Document Location
HM Government baseline personnel security standard	https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

9 Glossary

9.1 The following key terms are used in this document:

Term	Definition of term
Availability	Information and associated assets should be accessible to authorised users when required. The computer network must be resilient, and the Agency must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.
Confidentiality	Information should only be accessible to those authorised to access it, therefore preventing both deliberate and accidental unauthorised access to the Agency's information and proprietary knowledge and its systems, including its network(s), website(s), extranet(s), and e-commerce systems.
Integrity	This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data.
ISMS	A set of information security policies which address and look to minimise security risks of the Agency. A link to our security policies can be found here: Information Security Policies and Procedures.