Data Security and Protection Toolkit
Version 2
DCB0086 Change Specification

Published 29 May 2019

Information and technology
for better health and care

Copyright © 2019 Health and Social Care Information Centre.
The Health and Social Care Information Centre is a non-departmental body created by statute, also known as NHS Digital.

Amendment History:

Version	Date	Amendment History
0.1	27 February 2019	First draft
0.2	5 March 2019	Second draft – updated to reflect feedback and latest position on Cyber Essentials requirements
0.3	7 March 2019	Third draft – DHSC feedback incorporated
0.4	18 March 2019	Fourth draft – SME feedback incorporated
1	24 May 2019	Final version for publication

Approvals:

This document must be approved by the following:

Name	Organisation	Title / Responsibility	Date	Version
Daniel Taylor	NHS Digital	Associate Director of Data Security Centre Senior Responsible Owner	07 March 2019	0.2
Katie Farrington	Department of Health and Social Care	Director of Technology, Digital and Data Sponsor	07 March 2019	0.2

Data Coordination Board

This information standard (DCB0086) has been approved for publication by the Department of Health and Social Care under section 250 of the Health and Social Care Act 2012.

Assurance that this information standard meets the requirements of the Act and is appropriate for the use specified in the specification document has been provided by the Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Requirements Specification
- Implementation Guide
- Change Specification.

An Information Standards Notice (DCB0086 Amd 9/2019) has been issued as a notification of use and implementation timescales. Please read this alongside the documents for the standard.

The controlled versions of these documents can be found on the NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 29 May 2019

Copyright © 2019 Health and Social Care Information Centre.

Contents

Copyright © 2019 Health and Social Care Information Centre.

1. Overview

This Change Specification outlines the key differences between the Data Security and Protection (DSP) Toolkit version 1 (2018-19) and the DSP Toolkit version 2 (2019-2020).

This document should be read in conjunction with the DSP Toolkit Requirements Specification (specifically Appendix 1 – Assertions and Evidence items) and Implementation Guidance.

2. Definition

The DSP Toolkit is an online tool that enables organisations to measure their performance against data security and information governance requirements set by the Department of Health and Social Care.

The Toolkit has been developed in response to The NDG Review (Review of Data Security, Consent and Opt-Outs)[1] published in July 2016 and the government response published in July 2017.

The Data Security and Protection Toolkit is the successor framework to the IG Toolkit.

3. Guidance by user group

In accordance with the requirements of the Government Digital Service, the design and content of the DSP Toolkit have been developed to ensure the system is easy to use. The solution is designed to enable most users to be able to complete and publish an assessment without reference to detailed guidance documentation. The system has been designed after consultation with various Trusts and organisations and it substantially reduces the burden on organisations completing the toolkit in comparison with the predecessor system, the Information Governance Toolkit.

Guidance materials are made available via the DSP Toolkit Help pages: https://www.dsptoolkit.nhs.uk/Help. As far as reasonably possible sector specific guidance will be avoided but language which is suitable for all sectors has been included, tested with users and updated following consultation.

For more information, please refer to Implementation Guidance.

[1] https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

Copyright © 2019 Health and Social Care Information Centre.

4. Statement of all changes to the published Requirements Specification

4.1 DSP Toolkit version 2 – overview of changes

The DSPT Standard is reviewed annually. The 2019-20 standard is not a step change in the way the 2018-19 toolkit change was, but builds on the work and learning from 2018-19. Changes have been made in in order to:

- incorporate "Cyber Essentials" and the Minimum Cyber Security Standard (MCSS) for relevant organisations;
- incorporate key elements of the Network and Information Systems (NIS) Regulations 2018 Cyber Assessment Framework (CAF) for relevant organisations as advised by the National Cyber Security Centre;
- respond to lessons learned from the first year of the DSP Toolkit;
- improve the targeting of requirements to different categories of organisations; and,
- rationalise some of the General Data Protection Regulation (GDPR) evidence items which are now considered "business as usual".

4.2 DSP Toolkit changes – rationale and examples

To ensure high data security standards are in place for the organisations which process the highest risk information in the health and care system, the standards have been raised to match those required by government departments. Accordingly new evidence items such as the following have been added to ensure consistency with the Minimum Cyber Security Standard for example:

'Organisations understand which systems and services must be protected from cyber threat and have proportionate monitoring solution to detect cyber events.'

The Lessons learned review of the WannaCry Ransomware Cyber Attack from February 2018 recommended that all NHS organisations (Trusts) move towards Cyber Essentials PLUS, as recommended by the National Cyber Security Centre (NCSC). The DSP Toolkit standard for NHS Trusts has been uplifted to reflect this.

As part of the implementation of the Networks and Information Systems (NIS) Regulations, DHSC was appointed the 'Competent authority' and identified NHS Trusts as providers of essential services covered by the NIS Regulations. DHSC, in conjunction with advice from NCSC, has recommended three areas to strengthen the DSPT to support compliance with the NIS Regulations: privileged access controls, logging of data to support incident management, and backups. For example, the following evidence item has been added to cover backups:

'Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.'

The DSP Toolkit has been in place for organisations since April 2018. NHS Digital has reviewed the interim submissions competed by NHS Trusts and Arm's Length Bodies and picked a random sample of published assessment for interview and deep dive. Helpdesk queries and feedback submitted through the DSP toolkit has also been considered. The feedback on draft requirements for 2019-20 has been gathered from users of the standard

Copyright © 2019 Health and Social Care Information Centre.

both through direct engagement with users and through seeking comments via a news item on the DSP Toolkit.

In response to this feedback and analysis, wording of many evidence items has been improved to ensure requirements are clear and explicit. The following examples are provided:

2018-19 Requirement	2019-20 Requirement
Who are your staff with responsibility for data protection and/or security?	List the names and job titles of your key staff with responsibility for data protection and/or security.
Transparency information is published and available to the public.	How is transparency information (e.g. your Privacy Notice) published and available to the public?
Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.	Have at least 95% of all staff completed their annual Data Security awareness training in the period 1 April to 31 March?

In 2018-19, the DSP Toolkit standard varied according to organisation type and was broadly categorised as “Large”, “Small” and “GP”, mapped to organisation type/sector. This has led to some contradictions where a small company working with the NHS shredding paper waste would be categorised as a “large” as it was classed as a company, but a large care home organisation would be categorised as “small” as it is a social care organisation.

For 2019-20 the DSP Toolkit is simplified into

Category 1: NHS trusts

Category 2: Arm’s Length Bodies, CCGs and CSUs

Category 3: All other sectors (which do not fall under category 1, 2 or 4).

Category 4: GP Practice.

As the DSP Toolkit 2018-19 (version 1) was issued before GDPR came into force, it included evidence items that supported GDPR preparations. As GDPR has moved towards business as usual, these have now been incorporated in more general evidence items. For example, the evidence item:

There is an updated subject access process to meet shorter GDPR timescales.

is not included in version 2 (2019-20) and is consolidated into general evidence of policies and procedures.

The updates to the DSPT 2019-20 standard have led to an increase from 100 to 116 mandatory evidence items for NHS Trusts. This is due to additional evidence items being added to cover Cyber Essentials, MCSS and key NIS/CAF requirements. This has been balanced partially by a consolidation of GDPR requirements within the toolkit. The consolidation of GDPR requirements has led to a reduction in the evidence items for smaller organisations. A comparative breakdown is provided in the table below:

Copyright © 2019 Health and Social Care Information Centre.

	Category 1	Category 2	Category 3	Category 4
Mandatory Evidence items 18-19	100	100	70	52
Total Evidence Items 18-19	149	149	131	91
Mandatory Evidence items 19-20	116	106	56	42
Total Evidence Items 19-20	179	157	115	61

4.3 DSP Toolkit version 1 and 2 comparison

Appendix A provides an overview of requirements of the previous iteration of the Data Security and Protection Toolkit (2018-19 version 1). The table identifies equivalent areas in the DSP Toolkit standard for 2019-20 (version 2) and any elements which will no longer fall within the scope of the DSP Toolkit.

5. Change control during 2019-20

System refinements and new functionality will be deployed throughout 2019-20. Details of these changes will be set out within the "System changes and release notes" page on the DSP Toolkit: https://www.dsptoolkit.nhs.uk/News/1 . Material changes to the wording in the standards themselves will only be made in exceptional circumstances, such as where new legislation amends the requirement. This would be communicated to the users via email to those directly affected and set out within the "Standard changes and release notes" page on the DSP Toolkit help page.

Appendix A – DSP Toolkit 2018-19 (version 1) to 2019-20 (version 2) mapping

This is made available as a separate Excel document on the NHS Digital website: http://www/digital.nhs.uk/isce/publication/dcb0086

Copyright © 2019 Health and Social Care Information Centre.