

Data Security and Protection Toolkit Change Specification

Published 8 March 2018

Information and technology
for better health and care

Amendment History:

Version	Date	Amendment History
0.1	14/12/2017	First draft
0.2	15/01/2018	Amendments after receiving DSAS comments Author – Andrew Cooper
0.3	16/01/2018	Helpdesk information update
0.4	17/01/2018	Amendments after receiving DSAS final comments
0.5	23/01/2018	Amendments from reviewers Author – Andrew Cooper
1.0	08/03/2018	Final version for publication

Approvals:

This document must be approved by the following:

Name	Organisation	Title / Responsibility	Date	Version
Catherine O'Keeffe	NHS Digital	Director of Information Governance, Burden & Audit. SRO	19/01/2018	0.5
Daniel Taylor	NHS Digital	Director of Data Security Centre	19/01/2018	0.5
Katie Farrington	Department of Health and Social Care	Director of Digital and Data Sponsor	23/01/2018	0.5

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 58/2017) 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: 8 March 2018.



This information is licensed under the Open Government Licence v3.0. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/> or write to the Information Policy Team, The National Archives, Kew, Richmond, Surrey, TW9 4DU.

Contents

1. Overview	5
2. Definition	5
3. Helpdesk	5
4. Guidance by user group	6
5. Statement of all changes to the published Requirements Specification	6
5.1 IG Toolkit comparison – Overview	6
5.2 IG Toolkit Equivalence	7
6. Change control during 2018/19	7
Appendix A - IG Toolkit to DSP Toolkit Mapping	7

1. Overview

The DSP Toolkit is the successor framework to the IG Toolkit. This Change Specification outlines the key differences between the IG Toolkit (version 13, the last approved standard) and the DSP Toolkit.

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 Data Security and Protection (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. Helpdesk

Users should raise all incidents and support requests with the DSP Toolkit helpdesk. Support requests can be raised by telephone (9.00 – 17.00 on weekdays) or by email. Contact details are available from the help menu of the DSP Toolkit: www.dsptoolkit.nhs.uk.

Target service levels for the helpdesk (and service availability) are summarised below:

Description	Target
Total supported service availability (excluding planned downtime)	98%
Period of planned downtime	Maximum of 10 working days per annum
Incident response	95% within 4 working days
Incident resolution	95% within 5 working days
Restoration of full production service to failover infrastructure	Within 4 hours

An incident or support request may pass from 1st to 2nd to 3rd line support teams within these timescales. From a user's perspective it is one incident or support request raised and dealt with in the timescales outlined.

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

4. 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. There was a need for complete overhaul of the old toolkit as the new system aligns with the new standards as listed at section 2.

Guidance materials are made available via the DSP Toolkit Help pages: www.dsptoolkit.nhs.uk. As far as reasonably possible sector specific guidance will be avoided but language which is suitable for sectors has been included, tested with users and updated to following consultation. Language has been updated so the DSP toolkit aligns both with the NDG data security standards and GDPR which reduces the sector specific language.

For more information, please refer to Implementation Guidance.

5. Statement of all changes to the published Requirements Specification

5.1 IG Toolkit comparison – Overview

The DSP Toolkit is a new standard. No prior DSP Toolkit Requirements Specification exists.

The DSP Toolkit is the successor framework to the IG Toolkit. A summary of the key differences between these two standards is provided below:

- The requirements of the Data Security and Protection Toolkit are designed to encompass the 10 NDG Data Standards.²
- The requirements of the Data Security and Protection Toolkit support key requirements under the General Data Protection Regulation (GDPR), identified in the NHS GDPR Checklist³.
- The IG Toolkit assessed performance against three levels 1, 2 and 3. Organisations were required to evidence compliance with (at least) level 2 for all elements of their assessment. The Data Security and Protection Toolkit does not include levels, and instead requires compliance with assertions and (mandatory) evidence items.
- The Assertions and Evidence items within the DSP Toolkit are designed to be concise and unambiguous. Documentary evidence is only requested where this adds value.
- Some evidence items will not be required where an organisation uses NHSmail, or has in place an existing relevant standard (Cyber Essentials PLUS, ISO 27001, Public Service Network Information Assurance).

Please refer to the Requirements Specification for more information on the DSP Toolkit standard.

² As defined in the National Data Guardian “Review of Data Security Consent and Opt Outs” July 2016

³ NHS GDPR Checklist <https://digital.nhs.uk/information-governance-alliance/resources/technology>

5.2 IG Toolkit Equivalence

Appendix A provides an overview of key requirements of the IG Toolkit. The table identifies equivalent areas in the DSP Toolkit standard and any elements which are not within the scope of the DSP Toolkit.

The following requirements of the DSP Toolkit were not within the scope of the IG Toolkit:

- Leaders and Board Members receive suitable data security and protection training
- Organisations undertake process reviews to identify and improve processes which have caused breaches or near misses
- Organisations must act on CareCERT alerts and notifications
- Organisations must complete a specific business continuity test for data security
- Organisations must survey their software for unsupported systems
- Organisations must ensure all networking components have had their default passwords changed
- Large organisations must ensure their web applications are secure against OWASP top 10 vulnerabilities
- Large organisations must undertake a penetration test annually
- Large organisations must flag to NHS Digital, any suppliers with significant issues complying with the NDG Standards

6. Change control during 2018/19

System refinements and new functionality will be deployed throughout 2018/19. Details of these changes will be set out within the “System changes and release notes” page on the DSP Toolkit help page. 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.

Throughout 2018/19 development and SME resource is available to develop the standard and ensure significant changes can be incorporated into future versions of the standard such as GDPR and NIS.

Appendix A - IG Toolkit to DSP Toolkit Mapping

Please refer to separate file: **IG Toolkit to DSP Toolkit Mapping.pdf** which has been published on the DCB publication page: www.content.digital.nhs.uk/isce/publication/dcb0086