Department for Education

Educational and children's social care professionals DPS

Enhanced security schedule

March 2016

Contents

1. Definitions

In this schedule, unless the context otherwise requires, the following words have the meanings given to them below:

Authority: the Secretary of State for Education.

Authority Data: any data or information owned or retained in order to meet the Authority's business objectives and tasks including:

(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media and which are:

i. given to the Supplier by or on behalf of the Authority; or

ii. which the Supplier is required to generate, process, store or transmit pursuant to the Contract

(b) any Personal Data for which the Authority is the Data Controller.

BPSS: the HMG Baseline Personnel Security Standard for Government employees**.**

CESG: the information security arm of GCHQ;

Contract: the call-off terms and conditions entered into by the Supplier and the Authority into which this schedule is incorporated.

Cyber Essentials Scheme: the scheme backed by Government and industry to protect organisations from common cyber attacks, the details of which are available at:

www.gov.uk/government/publications/cyber-essentials-scheme-overview

Data Controller: has the meaning given to it in the DPA.

DPA: means the Date Protection Act 1998.

FIPS 140-2: the federal information processing standard titled "Security Requirements for Cryptographic Modules.

GSCP: the security classification policy of the United Kingdom government.

Incident: a situation which causes, or might cause, a disruption to the Services, loss, emergency or crisis.

ISO 22301: the international standard for business continuity management.

ISO/IEC 27001: the International Standard for Information Security Management Systems.

ISO/IEC 27002: the International Standard describing the Code of Practice for Information Security Controls.

Personal Data: has the meaning given to it in the DPA.

Security Health Check: an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on an IT system.

Services: means the services to be provided under the Contract.

Supplier: the supplier registered on the DPS who has accepted an Order.

2. Authority Data

2.1 The Supplier shall:

(a) have achieved and shall maintain independent certification to ISO/IEC 27001 and ISO/IEC 27002. The former must have a scope relevant to the Services and must be approved by the Authority;

(b) achieve and retain appropriate certification under the Cyber Essentials Scheme;

(c) keep Authority Data separate from Supplier data on the Supplier's IT system so that it can be identified and securely deleted if required by the Authority;

(d) have entry control mechanisms to premises and sensitive areas and separate logical access controls to its IT systems to ensure only authorised personnel have access to Authority Data;

(e) have technical protection for Authority Data including anti-virus software, firewalls, security updates and current patching regimes for anti-virus solutions, user-access controls and audit logs of system use;

(f) electronically transfer Authority Data across public space or the internet only if the Authority Data is protected via encryption certified to at least FIPS 140-2 standard or equivalent;

(g) store Authority Data on portable devices only if necessary in order to deliver the Services;

(h) store Authority Data on portable removable media only if necessary in order to deliver the Services and if the media are encrypted at least to FIPS 140-2 standard or equivalent;

(i) keep all removable media and hardcopy documents containing Authority Data secure when not in use and destroy them when no longer required using either a cross-cut shredder or a professional secure waste paper organisation;

(j) keep Authority Data contained in hard copy documents under cover when they are hand-carried;

(k) at the end of the Contract destroy or securely sanitise all Authority Data held by the Contractor in accordance with Authority policy using a CESG approved method or as instructed by the Authority;

(l) limit access to Authority Data to those of its staff who need access in order for the Supplier to perform the Services and who have the appropriate security clearance as required by the Authority which shall be at least equivalent to the BPSS;

(m) hold Authority Data outside the United Kingdom only with the Authority's prior written consent;

(n) ensure that any IT systems and hosting environments used to hold Authority Data are subject to an independent Security Health Check using a CESG approved provider before the start of Service delivery and annually during the term of the Contract;

(o) provide a report to the Authority on each Security Health Check which includes details of any remedial work carried out;

(p) ensure that all its staff who handle Authority Data have annual awareness training in protecting information;

(q) promptly report any breaches of the obligations in this paragraph 2.1 to the Authority; and

(r) subject to paragraph 2.2 handle Authority Data in accordance with the GSCP security classification given to it by the Authority.

2.2 The Supplier may continue to use its existing protective marking scheme but shall map the GSCP against it to ensure the correct controls are applied to Authority Data.

3. Business Continuity

3.1 The Supplier shall have robust business continuity arrangements which conform to ISO 22301 including IT disaster recovery plans and procedures to ensure that delivery of the Services is not adversely affected if there is an Incident.

3.2 The Supplier shall test its business continuity arrangements at least annually and provide a written report to the Authority on results of the test and any actions recommended as a result of the test.

3.3 The Authority may audit the Supplier's compliance with the obligations set out in this schedule at any time on reasonable notice to the Supplier.

Department for Education

© Crown copyright 2016

This publication (not including logos) is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

To view this licence:

visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3

email psi@nationalarchives.gsi.gov.uk

write to Information Policy Team, The National Archives, Kew, London, TW9 4DU

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DFE-00077-2016

Follow us on Twitter: @educationgovuk

Like us on Facebook: facebook.com/educationgovuk