



Department
for Education

Educational and Children's Social Care DPS

Data Handling and Security Standards

January 2021

Contents

Departmental Security Standards for Business Services and ICT Contracts – Terms and Definitions	3
Department’s Security Standards Clause	7

Departmental Security Standards for Business Services and ICT Contracts – Terms and Definitions

BPSS, Baseline Personnel Security Standard

means the [Government's HMG Baseline Personal Security Standard](#).

CCSC, Certified Cyber Security Consultancy

the [National Cyber Security Centre's \(NCSC\)](#) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards.

CCP, Certified Professional

a [NCSC scheme](#) in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession.

CPA, Commercial Product Assurance [formerly called “CESG Product Assurance”]

an [‘information assurance scheme’](#) which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.

Cyber Essentials, Cyber Essentials Plus

Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of [certification bodies](#) that can be approached for further advice on the scheme.

Data, Data Controller, Data Protection Officer, Data Processor, Personal Data, Personal Data requiring Sensitive Processing, Data Subject, Process, Processing

shall have the meanings given to those terms by the Data Protection Act 2018.

Department's Data, Department's Information

is any data or information owned or retained in order to meet departmental 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) supplied to the Contractor by or on behalf of the Department; or

(ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or

(b) any Personal Data for which the Department is the Data Controller;

DfE, Department

means the Department for Education.

Departmental Security Standards

means the Department's security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.

Digital Marketplace / G-Cloud

means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.

End User Devices

means the personal computer or consumer devices that store or process information.

Good Industry Practice, Industry Good Practice

means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.

Good Industry Standard, Industry Good Standard

means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.

GSC, GSCP

means the [Government Security Classification Policy](#) which establishes the rules for classifying HMG information.

HMG

means Her Majesty's Government.

ICT

means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution.

ISO/IEC 27001, ISO 27001

is the International Standard for Information Security Management Systems Requirements

ISO/IEC 27002, ISO 27002

is the International Standard describing the Code of Practice for Information Security Controls.

ISO 22301

is the International Standard describing for Business Continuity

IT Security Health Check (ITSHC), IT Health Check (ITHC), Penetration Testing

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

Need-to-Know

means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.

NCSC

The [National Cyber Security Centre](#) (NCSC) is the UK government's National Technical Authority for Information Assurance.

OFFICIAL, OFFICIAL-SENSITIVE

the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP).

the term 'OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP.

RBAC, Role Based Access Control

A method of restricting a person's or process' access to information depending on the role or functions assigned to them.

Storage Area Network, SAN

means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.

Secure Sanitisation

means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.

[NCSC Guidance](#)

[Disposal of physical documents and hardcopy materials advice.](#)

Security and Information Risk Advisor, CCP SIRA, SIRA

means the Security and Information Risk Advisor (SIRA) is a role defined under the [NCSC Certified Professional \(CCP\) Scheme](#).

Senior Information Risk Owner, SIRO

means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.

SPF, HMG Security Policy Framework

means the definitive [HMG Security Policy](#) which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely.

Department's Security Standards Clause

1. The Contractor shall be aware of and comply the relevant [HMG security policy framework](#), [NCSC guidelines](#) and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of [Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - Action Note 09/14](#) dated 25 May 2016, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved, and will be expected to retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the services supplied to, or on behalf of, the Department.
3. Where clause 2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

4. The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
5. Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor's or sub-contractor's own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 14.
6. The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.

7. The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC). User credentials that give access to Departmental Data or systems shall be considered to be sensitive data and must be protected accordingly.
8. The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:
 - physical security controls;
 - good industry standard policies and processes;
 - malware protection;
 - boundary access controls including firewalls, application gateways, etc;
 - maintenance and use of fully supported software packages in accordance with vendor recommendations;
 - use of secure device configuration and builds;
 - software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
 - user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;
 - any services provided to the department must capture audit logs for security events in an electronic format at the application, service and system level to meet the department's logging and auditing requirements, plus logs shall be:
 - a. retained and protected from tampering for a minimum period of six months;
 - b. made available to the department on request.
9. The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.
10. The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.
11. The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found on NCSC's [guidance](#)

[page](#) and [End User Devices page](#).

12. Whilst in the Contractor's care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term 'lock and key' is defined as: "securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user's sole control and to which they hold the keys".

13. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term 'under cover' means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

14. In the event of termination of contract due to expiry, liquidation or non-performance, all information assets provided, created or resulting from the service shall not be considered as the supplier's assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 2.15.
15. In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-contractor shall protect the Department's information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

16. Access by Contractor or sub-contractor staff to Departmental Data, including user credentials, shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted. Any Contractor or sub-contractor staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact.
17. All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.
18. The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
19. Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data, including user credentials, used or handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department’s nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

20. The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
21. The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.
22. The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor's, and any sub-contractors', compliance with the clauses contained in this Section.
23. The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. This will include obtaining any necessary professional security resources required to support the Contractor's and sub-contractor's security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.
24. Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department's expectation is that the Contractor shall provide written evidence of:
- Compliance with HMG Minimum Cyber Security Standard.
 - Any existing security assurance for the services to be delivered such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
 - Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.

- Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.

25. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.



Department
for Education

© Crown copyright 2021.

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



Follow us on Twitter:
[@educationgovuk](https://twitter.com/educationgovuk)



Like us on Facebook:
facebook.com/educationgovuk