Information Security Responsibilities for Contractors Handling 'OFFICIAL' Information outside NDA Premises

Nuclear Decommissioning Authority

IPPR01-TAC09

Rev 1 January 2016

1. INTRODUCTION

1.1 Throughout this document, the "Authority" is the Nuclear Decommissioning Authority (NDA), a Subsidiary of the NDA or a Site Licence Company (SLC)

1.2 All information created, processed, used, stored or shared by or on behalf of the Authority in the conduct of its business is OFFICIAL information: It has intrinsic value and requires an appropriate degree of protection.

2. SCOPE

2.1 Everyone who works with OFFICIAL information (including suppliers) has a duty of confidentiality and a responsibility to safeguard any such information or data that they have access to. OFFICIAL information must be handled with care to prevent loss or compromise.

2.2 Accidental or deliberate compromise, loss or misuse of certain OFFICIAL information may, under certain circumstances, constitute a criminal offence (e.g. under the Official Secrets Acts of 1911 to 1989, or the Data Protection Act 1998).

2.3 Individuals are personally accountable for protecting all OFFICIAL information in their care and must be provided with guidance about security requirements. This document provides Contractors with the requirements for managing OFFICIAL information; additional information can be found in the Government's Security Policy Framework and Security Classifications documents.

2.4 The Contractor shall ensure that every person who requires access to OFFICIAL information to enable the Contractor to deliver the service(s) the Authority has contracted it to supply is informed of and complies with the requirements established in this document.

3. OFFICIAL INFORMATION

3.1 The Authority operates a positive marking policy. Under the Government Security Classifications scheme, all information that is created, processed, used, stored or shared by or on behalf of the Authority is to be given a classification marking according to its content and/or sensitivity.

3.2 Occasionally information or documents may be received from other parties which do not bear a classification marking. The Contractor shall, for the avoidance of doubt, treat such unmarked information as OFFICIAL.

3.3 The security requirements and restrictions do not apply to information that has been published or otherwise been made widely available to the general public by the Authority or any of their predecessor organisations, or which the Contractor is required or directed to release to:

a) individuals or groups of individuals, who are not under contract (directly or indirectly) to the Authority, or to the public in general, in order to deliver the service(s) the Authority has contracted it to provide; or

b) a third party under a statutory requirement (e.g. the Data Protection Act 1998 or the Freedom of Information Act 2000).

("Release", in the context of paragraph 3.3, means to disclose without any requirements relating to its subsequent protection).

4. CONTROLS FOR THE PROTECTION OF OFFICIAL INFORMATION

4.1 The Contractor shall apply any controls specified in handling advice provided with any OFFICIAL information received, or which are otherwise stipulated by the Authority.

4.2 The Contractor shall handle all information with the appropriate degree of care to prevent loss, compromise, or inappropriate access. "Inappropriate access" means access by a person other than a person who requires access to that information for the Contractor to deliver the service(s) the Authority has contracted it to provide. "Appropriate degree of care" means:

a) the baseline controls specified in this document, or;
b) additional controls that the Contractor considers more appropriate, taking into account the sensitivity of the OFFICIAL information in question and the need to protect it from compromise by attackers with bounded capabilities and resources.

4.3 The Contractor shall, when creating, modifying, processing or annotating OFFICIAL information, consider whether any additional controls are likely to be necessary to protect it. Such considerations shall always take account of the sensitivity and the need to protect it from compromise by attackers with bounded capabilities and resources.

4.4 "Attackers with bounded capabilities and resources" include single-issue pressure groups, private investigators, competent individual hackers, 'hacktivists', individuals that might commit theft, and any other individuals or groups presenting an equivalent level of threat to the Authority.

4.5 If the Contractor identifies information as particularly sensitive, with a clear and justifiable need to reinforce the 'need to know' (for example; sensitive personal data, commercial or financial data), a conspicuous marking of OFFICIAL-SENSITIVE shall be considered. In such cases the Contractor shall seek the advice of the Authority.

4.6 When considering the sensitivity of OFFICIAL information, the Contractor shall take into account the degree to which it's compromise or loss would be likely to:

a) have damaging consequences for an individual (or individuals), the Authority, UK Government or any other organisation, if lost, stolen or published in the media;
b) cause significant or substantial distress to individuals or a group of people;
c) breach undertakings to maintain the confidentiality of information provided by third parties;
d) breach statutory restrictions on the disclosure of information (including those under the Official Secrets Acts 1911 to 1989, the Data Protection Act 1998 and the Anti-terrorism, Crime and Security Act 2001);
e) undermine the proper management of the public sector and its operations;
f) disrupt national operations;
g) impede the development or operation of UK Government policies; or
h) substantially undermine the financial viability of major organisations.

4.7 When assessing the sensitivity of OFFICIAL information, consideration shall not be limited to the implications of its compromise or loss in isolation; but must take into account the effects of the aggregation, accumulation and association of the OFFICIAL information in question with other OFFICIAL information handled by the Contractor.

4.8 Where the Contractor considers additional controls to protect OFFICIAL information from inappropriate access, those further controls will be specified in handling advice provided with the OFFICIAL information in question. Such advice shall describe the particular sensitivities of the information and provide meaningful guidance on how it should be handled. It should be presented in accordance with the following formula:
<the particular sensitivity of the information> <what the handler is allowed to do with the information> <what the handler needs to do to ensure it is given the appropriate level of protection>

4.9 The handling advice shall be displayed in a place where it would be most obvious to the handler (e.g: top of the first page of a document or email containing the information).

5. BASELINE CONTROLS FOR OFFICIAL INFORMATION

Access and Personnel Security

5.1 The Contractor shall ensure that every person who requires access to OFFICIAL information for the Contractor to deliver the service(s) the Authority has contracted it to supply has been subject to identity, nationality and right to work in the UK checks. If the Contractor wishes to employ any

non-UK nationals on the contract he shall, prior to engaging the non-UK national, consult with the Authority as further checks and approvals may be needed.

5.2 Where the Contractor's employees require regular access to the Authority's premises or access to the Authority's IT network those persons shall as a minimum be subject to Baseline Personnel Security Standard (BPSS) security checks.

5.3 In respect of the Contractor's employees already holding a security clearance, but where the Authority is not the Vetting Authority, the Contractor shall prior to any work commencing provide the Authority's Contract Lead with the employee's name, date of birth, and the contact details of the relevant vetting authority.

5.4 "Relevant vetting authority" is, in relation to employees described in paragraph 5.3, the vetting authority that carried out the personnel security check or currently holds the security clearance.

5.5 "Vetting authority" means an organisation which is either formally approved by the Office for Nuclear Regulation (ONR) to initiate and manage BPSS checks or a body authorised to carry out equivalent or higher levels of checks, security clearance or vetting (e.g. a police authority or Defence Business Services).

Information Technology (IT) and Cyber Security

5.6 The Contractor shall ensure that any IT network, part of an IT network, or IT equipment used to create, process, use, store or share OFFICIAL information is either:

a) accredited by an approved third party (ONR, Ministry of Defence (MOD) etc.) or NDA, to HMG IA Standards No. 1 and 2; or is:

b) used and maintained in accordance with the five "technical requirements" of the UK Government's 'Cyber Essentials' Scheme. (Cyber Essentials and Cyber Essentials Plus have been designed to provide 'light-touch' assurance, achievable at low cost)

5.7 The Contractor shall demonstrate to the Authority's satisfaction that the "technical requirements" are being met through independent verification at least once every 12 months. Verification shall be equivalent to the Cyber Essentials Assurance Framework level specified by the Authority in the Contract Letter (Cyber Essentials or Cyber Essentials Plus). Verification may be gained through existing certification to other information security standards, such as ISO 27001:2013 or its successor(s).

5.8 The Contractor shall ensure that any mobile IT equipment (e.g. laptop, tablet, other mobile devices) or desk top computer located in domestic or residential premises which is used to create, process, use, store or share OFFICIAL information has full disk foundation grade encryption to Commercial Product Assurance (CPA)

5.9 The Contractor shall ensure that the deletion of OFFICIAL information from an IT network, part of an IT network, or IT equipment is carried out in accordance with HMG Information Assurance (IA) Standard No. 5 (Secure Sanitisation).

5.10 The Contractor shall ensure that any OFFICIAL information that the Authority requires to be deleted from an IT network, part of an IT network, or IT equipment is deleted in accordance with paragraph 5.8.

5.11 The Contractor shall ensure that any OFFICIAL information on an IT network, part of an IT network, or IT equipment will be deleted in accordance with paragraph 5.9 before the equipment in question is discarded or disposed of.

Electronic transmission and communication

5.12 OFFICIAL information may be transmitted by email over the Internet, as follows:

a) to provide additional protection the Contractor should consider additional handling instructions and encrypting the information using a file compression ('zip') application set to 256 bit AES encryption and a strong password. Passwords must be sent by a separate channel (e.g. text message, telephone call, royal mail post);
b) e-mail operating within the Egress Switch Secure Workspace system; or
c) subject to the Authority's prior written agreement, other commercially available means of transmitting or sharing information in electronic form (e.g. G-Cloud services).

Information in hard-copy or on removable, recordable media

5.13 The Contractor shall record OFFICIAL information onto portable media device (e.g. usb memory stick, CD/DVD) only if it is necessary for the Contractor to do so in order for it to deliver the service(s) that the Authority has contracted it to supply, and that all such devices are encrypted using approved encryption software (see paragraph 5.7).
N.B. under no circumstances should any portable media be connected to the Authority's IT network without prior authorisation from the Authority's IT Security Manager and IT Manager.

5.14 The Contractor shall ensure that paper documents, records, etc. (or parts thereof) containing OFFICIAL information are photocopied or scanned into electronic form only if it is necessary for the Contractor to do so in order for it to deliver the service(s) that the Authority has contracted it to supply.

5.15 The Contractor shall ensure that all paper documents, records, etc., portable IT equipment (e.g. laptops, tablets) and portable digital media (e.g. memory sticks, CD ROMs) containing OFFICIAL information are stored in locked office furniture (e.g. desk drawer, cupboard, filing cabinet) within a secure building, when not in use. The key(s) to the office furniture must be securely held.

5.16 The Contractor shall ensure, when moving OFFICIAL information by hand that the information is not capable of being seen by anyone that would not be granted access to it. The Contractor should avoid OFFICIAL information being overlooked by others if it is being worked on whilst it is in transit and, when it is not being worked on, ensure it is obscured from sight by an opaque cover (e.g. a document should be carried in an envelope, a case or closed bag).

5.17 The Contractor shall ensure, when transmitting OFFICIAL information by post or courier that it is contained in a single, unused envelope or parcel wrapping and that a return address is provided on the back of the envelope or parcel. The outside of the envelope or parcel must NOT be marked OFFICIAL (or with any other marking that might convey the nature of the information it contains).

5.18 The Contractor shall not carry out bulk transfers of documents, records, etc. containing OFFICIAL information without having undertaken an assessment of the risks associated with the proposed method of transfer and having obtained the prior (written) authorisation of the relevant Information Asset Owner. Advice on the likely suitability of proposed methods of transfer and assessments of their risks may be sought from the Authority's Security Manager.

5.19 Once the Contractor no longer needs access to the OFFICIAL information in order to deliver the service(s) that the Authority has contracted it to supply, or to fulfil any other legal or contractual obligations (to the Authority or a third party), the Contractor shall ensure that, where the OFFICIAL information in question is contained in or on:

a) a paper document; the paper document is either returned to the Authority or shredded on the Contractor's premises in accordance with HMG Information Assurance (IA) Standard No. 5 (Secure Sanitisation) before being disposed of from the Contractor's premises;

b) a CD ROM or DVD; the CD ROM or DVD is either returned to the Authority or broken up (so as to make reconstitution unlikely) on the Contractor's premises, before being disposed of from the Contractor's premises;
c) an encrypted removable memory device; the OFFICIAL information in question is deleted from the device using commercially available secure-wipe software product under Commercial Product Assurance (CPA)
d) In respect of information destroyed by the Contractor, the Contractor shall provide the Authority with written confirmation that all of the Authority's material pertaining to the work the contractor was engaged for (and whether classified or not) has been destroyed.

Breaches and Incident reporting

5.20 Contractors must have a breach management system in place to aid the detection and reporting of inappropriate behaviours, enable disciplinary procedures to be enforced and assist with criminal proceedings.

5.21 Immediately upon it becoming known to the Contractor, any event involving the theft, loss, or significant inappropriate access to the Authority's OFFICIAL information, shall be reported to the Authority by the most expedient means.