|  |  |  |  |
| --- | --- | --- | --- |
| **Document Control Sheet** | | | |
| Author and Owner | | Matthew Collantine | |
| Document Path and Livelink number | | Livelink – QMS Live – S&CS  [35489581](http://ndahqewc01/livelink/llisapi.dll?func=ll&objaction=overview&objid=35489581) | |
| Version number | | V9 | |
| Status | | Live | |
| Version Publication date | | September 2022 | |
| Related QMS Documents | | SCPR13 | |
| Review Frequency and Date | | Annual  September 2023 | |
| Approved by and Date | | Matthew Collantine  September 2022 | |
| Distribution | | All NDA staff | |
| **Version** | **Date** | **Comments/Change** | **Author** |
| 6 | August 2020 | Review original IPPR01-TAC09 document, update and convert to the new procedure template  New number allocated to move into security area | Matthew Collantine |
| 7 | October 2020 | update to section 4.8 to align with the rest of the Policies and processes. | Paul Jacka |
| 8 | September 2021 | Reviewed and redated | Paul Jacka |
| 9 | Sept 2022 | Reviewed and dated | Paul Jacka |
| **Please note that the version of this document contained within the QMS is the only version that is maintained.**  Any printed copies should therefore be viewed as “uncontrolled” and as such, may not necessarily contain the latest updates and amendments. | | | |

1. Scope
   1. This procedure[[1]](#footnote-1) describes the responsibilities of handling NDA information to all staff including contractors.
   2. Everyone who works with OFFICIAL information (including Contractors) 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.
   3. 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. Responsibilities
   1. **NDA** - will require suppliers to demonstrate, evidence how every person who requires access to OFFICIAL information is informed and complies with the requirements established in this document.
   2. **The primary contractor** - is responsible for cascading these requirements to any sub-contractors it may work with and for ensuring the requirements are fully implemented. Primary contractors must obtain authority to employ sub-contractors from the Authority.
   3. **Individuals** - are personally accountable for protecting all OFFICIAL information in their care.
   4. **NDA Information Governance and Security Team** – When engaging with contractors this team may review, comment and request further clarification from any supplier to ensure NDA information is being protected accordingly.
   5. **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.
   6. **The Contractor shall** - apply any controls specified in handling advice provided with any OFFICIAL information received, or which are otherwise stipulated by NDA. Handle all information with the appropriate degree of care to prevent loss, compromise, or inappropriate access.
   7. **Contractors** - must have a breach management system in place.
3. Definitions

* 1. **OFFICIAL information** - All information created, processed, used, stored or shared by or on behalf of NDA in the conduct of its business is, at minimum OFFICIAL information: It has intrinsic value and requires an appropriate degree of protection.
  2. Throughout this document there will be reference to current legislations and acts, these include but not limited to; Official Secrets Acts of 1911 to 1989, Data Protection Act 2018 (DPA), UK General Data Protection Regulation (UK GDPR) ), Environmental Information Regulations (EIR) 2004 and the Freedom of Information Act 2000 (FoI).
  3. **Release of information** - “Release”, in this context, means to disclose without any requirements relating to its subsequent protection.
  4. **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) NDA has contracted it to provide.
  5. **Appropriate degree of care** – means:
* the baseline controls specified in this document, or;
* additional controls that the Contractor considers more appropriate, considering the sensitivity of the OFFICIAL information in question and the need to protect it from compromise by attackers with bounded capabilities and resources.
  1. **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 NDA.
  2. **Personnel security checks** – depending on the information level and sensitivity NDA may require those personnel to undergo additional security checks such as but not limited to; Baseline Personnel Security Standard (BPSS), National Security Vetting Clearance (SC).
  3. **Vetting Authority** – an organization which is either formally approved by the Office for Nuclear Regulation (ONR), police authority or Defence Business Services.

1. Content
   1. 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.
   2. 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 NDA or any of their predecessor organisations, or which the Contractor is required or directed to release to:

* individuals or groups of individuals, who are not under contract (directly or indirectly) to the Authority, or to the public in general, to deliver the service(s) the Authority has contracted it to provide; or
* a third party under a statutory requirement (e.g. the Data Protection Act 2018 (Including UK General Data Protection Regulation, Environmental Information Regulations (EIR) 2004 or the Freedom of Information Act 2000).
  1. 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 NDA.
  2. When considering the sensitivity of OFFICIAL information, the Contractor shall take into account the degree to which its compromise or loss would be likely to:
* have damaging consequences for an individual (or individuals), NDA, UK Government or any other organisation, if lost, stolen or published in the media;
* cause significant or substantial distress to individuals or a group of people;
* breach undertakings to maintain the confidentiality of information provided by third parties;
* breach statutory restrictions on the disclosure of information (including those under the Official Secrets Acts 1911 to 1989, the Data Protection Act 2018, Environmental Information Regulations (EIR) 2004 and the Anti-terrorism, Crime and Security Act 2001);
* undermine the proper management of the public sector and its operations;
* disrupt national operations;
* impede the development or operation of UK Government policies; or
* Substantially undermine the financial viability of major organisations.
  1. 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.
  2. 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>*

* 1. 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).

**Baseline controls for OFFICIAL Information**

**Access and Personnel Security**

* 1. Anyone requiring access to OFFICIAL information only, specifically excluding access to that classified as OFFICIAL-SENSITIVE, and who does not need unescorted access to NDA premises, shall be subject to pre-employment checks that include as a minimum: HMG Baseline Personnel Security Standard (BPSS). Suppliers must inform NDA where the nationality (including dual or former nationality) of any person falls outside of countries in the EEA, NATO, Japan or a country which shares the same Head of State as the UK prior to the individual in question being given any access to information.
  2. Any supplier staff/sub-contractors requiring access to OFFICIAL-SENSITIVE information shall be subject to pre-employment checks that include the HMG Baseline Personnel Security standard as a minimum. Under Nuclear Regulation NDA can only accept BPSS clearances carried out by “ONR recognised Signing Authorities”, requirements should be confirmed with the NDA Vetting Team prior to commencing any clearance checks and Supplier staff will be required to undergo the NDA Security Induction before accessing OFFICIAL-SENSITIVE information.
  3. A Baseline Personnel Security Standard (BPSS) shall be required as a minimum if an NDA pass or IT network account is required.
  4. Typically where contracts involve access to Secret SNI information Supplier staff shall require National Security Vetting clearance at SC level and Supplier staff will be required to undergo the Buyer Security Induction.
  5. There may be some instances where NDA require higher level clearances, where this incidence occurs NDA will stipulate this to the Supplier in writing, usually during Tender stage of the procurement process.
  6. 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.

**Information in hard-copy or on removable, recordable media**

* 1. 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. [[2]](#footnote-2)
  2. The Contractor shall ensure that all paper documents, records, etc., portable IT equipment (e.g. laptops, tablets, smart phones) 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. [[3]](#footnote-3)
  3. 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).
  4. 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. 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 NDA’s Security Manager.
  6. Once the Contractor no longer needs access to the OFFICIAL information to deliver the service(s) that NDA has contracted it to supply, or to fulfil any other legal or contractual obligations (to NDA or a third party), the Contractor shall ensure that, where the OFFICIAL information in question is contained in or on:
* a paper document; the paper document is either returned to NDA 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;
* a magnetic or optical media; the information or media should either be returned to NDA, destroyed or sanitised at the Contractor’s premises in accordance with HMG Information Assurance (IA) Standard No. 5 (Secure Sanitisation);
* In respect of information destroyed by the Contractor, the Contractor shall provide NDA with written confirmation that all of NDA’s material pertaining to the work the contractor was engaged for (and whether classified or not) has been destroyed.

**Breaches and Incident Reporting**

* 1. 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.
  2. Immediately upon it becoming known to the Contractor, any event involving the theft, loss, or significant inappropriate access to NDA’s OFFICIAL information, shall be reported to NDA by the most expedient means.
  3. Email breach and incident reports to “security.reporting@nda.gov.uk”

1. Documentation

|  |  |  |  |
| --- | --- | --- | --- |
| **Document reference** | **Document type** | **Function owner** | **Paper (location) or electronic** |
|  |  |  |  |
|  |  |  |  |

1. This document was previously known as TAC09. [↑](#footnote-ref-1)
2. Consideration should be given to photocopier devices, particularly those on leases, which could contain hard drives. These hard drives can contain sensitive corporate information. [↑](#footnote-ref-2)
3. Other physical security requirements can be found within SCPR13 “*Technical requirements for Contractors working in non-NDA locations (Official Classification)”* [↑](#footnote-ref-3)