|  |
| --- |
| **Document Control Sheet** |
| Author and Owner | Matthew Collantine |
| Document Path and Livelink number | Livelink – QMS Live – S&CS[35486772](http://ndahqewc01/livelink/llisapi.dll?func=ll&objaction=overview&objid=35486772) |
| Version number | V7 |
| Status  | Live |
| Version Publication date | September 2022 |
| Related QMS Documents | ITP09, SCPR11 |
| Review Frequency and Date | Annual September 2023 |
| Approved by and Date | Matt Shreeve Sept 2022 |
| Distribution  | All NDA staff |
| **Version** | **Date** | **Comments/Change** | **Author** |
| 5 | August 2020 | Review original TAC11 document and update. Change to new procedure template. | Matthew Collantine |
| 6 | August 2021 | Reviewed and amended versions | Paul Jacka |
| 7 | September 2022 | Review and date | 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 document[[1]](#footnote-1) provides requirements to suppliers and contractors working for, and on behalf of, the Nuclear Decommissioning Authority’s Corporate Centre (NDA).
	2. All information created, processed, used, stored or shared by or on behalf of NDA in the conduct of its business is, at a minimum, OFFICIAL information: It has intrinsic value and requires an appropriate degree of protection.
2. Responsibilities
	1. 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 NDA.
	2. This document is for those using a business-issued device; it does not apply to personal home computers.
	3. You must not use your own personal computer (or anyone else’s) to work on OFFICIAL information or projects unless you have prior approval from NDA.
	4. Business-issued devices are assumed to be provided solely for work purposes, and only by people authorised by the business itself.
	5. Suppliers to NDA should hold Cyber Essentials or Cyber Essential Plus certification, or be able to satisfy NDA that they meet the requirements of Cyber Essentials or Cyber Essential Plus through technically competent independent verification[[2]](#footnote-2).
	6. Where this document is not explicit in its requirements it is expected that good business practices should be implemented.
	7. The information being processed or stored is classified as OFFICIAL or OFFICIAL-SENSITIVE, but specifically excludes that information considered Sensitive Nuclear Information (SNI).
	8. Information considered to be OFFICIAL-SENSITIVE must always be transmitted and stored in an encrypted form.
	9. If you are planning to send or take OFFICIAL information overseas you must discuss it in advance with NDA.
3. Definitions
	1. The OFFICIAL-SENSITIVE caveat should not be confused with a separate classification; it is a tool to denote OFFICIAL information that is of a particular sensitivity but that can be managed on OFFICIAL systems and infrastructure.
	2. The loss, compromise or misuse of information marked with the OFFICIAL-SENSITIVE caveat has been assessed as being likely to have damaging consequences for an individual, an organisation or Her Majesty's Government more generally. Risk owners will typically require additional assurance that the need-to-know is strictly enforced, and there is a clear requirement to protect the confidentiality, integrity and availability of this information.
	3. OFFICIAL information will normally be protected using appropriately assured, commercially available security products and service offerings.
	4. Whilst these security products and service offerings cannot absolutely assure against the most sophisticated and determined threat actors, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access OFFICIAL information.
	5. Cryptographic protection at OFFICIAL should comply with good commercial practice. In practice, this means the use of algorithms and protocols that are approved by international public standards bodies.
4. Content

**ADDITIONAL TECHNICAL REQUIREMENTS FOR COMPUTING EQUIPMENT**

* 1. Strong passwords must be used to protect OFFICIAL information from unauthorised access.
	2. Whole-disk encryption must be installed and operational on laptops and desktop computers.
	3. Removable storage media (including, but not limited to, CD-ROMs, external hard-drives and USB memory keys) must be fully encrypted when used for OFFICIAL information.
	4. Your computer must not be left unattended in a public area at any time. Your computer should be screen-locked whenever you move away from it, and completely powered-down when left unaccompanied for longer periods of time.
	5. Users must have individual login accounts, which must not be shared.
	6. Users should adhere to “least privilege” principles for their login accounts.
	7. Elevated privilege user accounts (e.g. local admin) should not be used for general business activities.
	8. A current and up to date anti-virus solution must be installed.
	9. When a remote access, or virtual private network (VPN), solution is used it must be based on two-factor authentication (e.g. an RSA key fob and password, for example).
	10. When there remains no further legitimate requirement to retain OFFICIAL information it must be deleted.
	11. When a computer is ultimately disposed of, the hard drive must be sanitised (securely deleted) to clear any remaining NDA data in accordance with HMG Information Assurance Standard No 5 (IAS5) [[3]](#footnote-3).
	12. Only those authorised and cleared to work on OFFICIAL information should have access to the computer.
	13. The business must employ appropriate network segmentation and segregation to ensure the need-to-know principle is adhered to; only those who are authorised and with a genuine requirement should have access to OFFICIAL information.

**GENERAL REQUIREMENTS**

* 1. Unnecessary volumes of paper-based OFFICIAL information must not be stored or retained.
	2. Paperwork related to OFFICIAL information must be disposed of in accordance with HMG Information Assurance Standard No 5 (IAS5), or stored securely until you can bring it into an NDA office for secure destruction.
	3. Do not connect unauthorised or unknown devices to your laptop or desktop computer.
	4. Untrusted removable media must not be used in your computer, this is particularly important when receiving CD-ROMs or USB memory keys from unknown/untrusted sources. Unknown removable media can contain viruses and malware.
	5. Computers used for processing and storing OFFICIAL information must not be left visible in a vehicle at any time.
	6. Reasonable efforts should be made to protect your computer when not in use through the use of locked furniture and/or Kensington locks.
	7. No passwords or VPN tokens (e.g. RSA key fobs) are to be stored with the computer.
	8. Be aware that quantities of lower sensitivity information may pose an increased security risk when aggregated.
	9. If you have suffered a theft, loss or the potential of inappropriate access to information related to work with NDA you must let NDA know via the most expedited means.
	10. When travelling you should carry no more electronic or paper-based OFFICIAL information than is actually needed.

**PHYSICAL SECURITY REQUIREMENTS FOR OFFICES**

* 1. Proportionate physical security controls shall be implemented to prevent unauthorised access to locations where paper-based assets and ICT systems components are processed and stored. This shall include as a minimum but is not limited to:
* Lockable office space with good quality locks and control over keys or other means giving access to the office space.
* Lockable windows with good quality locks which should be closed and locked whenever the office is left unattended.
* Clear Desk procedure to be followed whenever the office is left unattended and at cease of work.
* A “Last Person Out” procedure, to be followed whenever the office is left unattended and at cease of work.
* Secure storage with control over keys or other means giving access to the storage.
* Segregated storage of hard copy records and information assets away from other client’s information.
* In shared office environments measures must be put in place to prevent unauthorised and inadvertent access from overviewing and overhearing.

**OFFICES IN THE HOME ENVIRONMENT**

* 1. The use of home office environments must be disclosed and approval for their use obtained in advance from NDA, as additional assurances may be required.
	2. The physical security requirements as outlined above for offices are equally applicable to offices in home environments.
1. Documentation

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

1. This document was previously known was TAC11. [↑](#footnote-ref-1)
2. Please see guidance note, "Cyber Essentials in the NDA", for further details. [↑](#footnote-ref-2)
3. Businesses without access to “HMG IA Standard No. 5 - Secure Sanitisation” can request further details from NDA. [↑](#footnote-ref-3)