Contractors working in non-NDA locations

Nuclear Decommissioning Authority

IPPR01-TAC11

Rev 1 July 2016

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.

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.

The level of assurance required for OFFICIAL classification is Foundation Grade, which will typically be provided by CESG's Commercial Product Assurance (CPA) scheme.

For OFFICIAL information the use of a CPA encryption product is strongly recommended, although organisations may also conduct other suitably-scoped assurance activities to provide further options. For information that is considered OFFICIAL-SENSITIVE the choice of a non-CPA product will need strong justification and prior agreement by the NDA.

Key principles

- 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 NDA.
- This is for those using a business-issued non-NDA device; it does not apply to personal home computers.
- You must not use your own personal computer (or anyone else's) to work on NDA information or projects.
- Business-issued devices are assumed to be provided solely for work purposes, and only by people authorised by the business itself.
- The business that issued the device must hold Cyber Essentials or Cyber Essential Plus certification, or be able to satisfy the NDA that they meet the requirements of Cyber Essentials or Cyber Essential Plus through technically competent independent verification.
- The information being processed or stored is classified as OFFICIAL or OFFICIAL-SENSITIVE, but specifically excludes that information considered Sensitive Nuclear Information (SNI).
- If you are planning to send or take NDA information overseas you must discuss it in advance with the NDA.

Nuclear Decommissioning Authority

IPPR01-TAC11

Rev 1 July 2016

Additional technical requirements for non-NDA issued equipment

- Strong passwords must be used to protect NDA information from unauthorised access.
- Whole-disk encryption must be installed and operational on laptops and desktop computers.
- Removable storage media (including, but not limited to, CD-ROMs, external hard-drives and USB memory keys) must be fully encrypted when used for NDA information.
- 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.
- Users must have individual login accounts, which must not be shared.
- Users should adhere to “least privilege” accounts where possible.
- Elevated privilege user accounts (e.g. local admin) should not be used for general business activities.
- A current and up to date anti-virus solution must be installed.
- 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).
- When there remains no further legitimate requirement to retain NDA information it must be deleted.
- 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 (IS5).
- Only those authorised and cleared to work on the NDA’s information must have access to the computer.
- 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 the NDA’s information.

General requirements

- Unnecessary volumes of paper-based NDA information must not be stored or retained.
- Paperwork related to NDA information must be disposed of in accordance with the relevant HMG Information Assurance Standard (IS5), or stored securely until you can bring it into an NDA office for secure destruction.
- Do not connect unauthorised or unknown devices to your laptop or desktop computer.
- 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.
- Computers used for processing and storing NDA information must not be left unattended in a vehicle at any time.
- Reasonable efforts should be made to protect your computer when not in use through the use of locked furniture and/or Kensington locks.
- No passwords or VPN tokens (e.g. RSA key fobs) to be stored with the computer.

- Be aware that quantities of lower sensitivity information may pose an increased security risk when aggregated.
- If you have suffered a theft, loss or the potential of inappropriate access to information related to the NDA you must let the NDA know via the most expedited means.
- When travelling you should carry no more electronic or paper-based NDA information than is actually needed.

Physical security requirements for offices

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 (e.g. to standard “LPS 1175 SR 2”) 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 approved storage (e.g. to standard “EN 14450 S2”) with control over keys or other means giving access to the office space.
- 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

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