CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

PO & OA ANNEX I - Contract Security Clause for inclusion in RFPs and contracts involving NATO Restricted information

INTRODUCTION

1. This contract security clause is published by the Security Committee (AC/35) in support of NATO Security Policy, C-M (2002)49, and its supporting directives.

BACKGROUND

2. This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract. This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

3. This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

SECTION I – RESPONSIBILITY

4. Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by the Contracting Authority[1]. The SO shall also act as the point of contact with the Contracting Authority or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

SECTION II - PERSONNEL SECURITY

5. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the facility security officer.

SECTION III - PHYSICAL SECURITY

6. NR information shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet**,** or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone[2]).

7. NR information shall be handled in Administrative Zones or held under personal custody.

[1] Contracting Authority is NSPA

[2] An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones

SECTION IV - SECURITY of INFORMATION

Control and Handling

8. Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

9. Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5, second sentence.

Reproduction

10. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

Destruction Requirements

11. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

12. Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

13. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

14. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transmission

15. The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

(a) moved by postal or commercial services;
(b) carried by Contractor's personnel; or
(c) transported as freight by commercial services.

Release

16. NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

17. Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the Contracting Authority.

SECTION V - SUB-CONTRACTING

18. Sub-contracts shall not be let without the prior approval of the Contracting Authority.

19. Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

20. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

International Visits

21. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

SECTION VI - HANDLING OF NATO RESTRICTED INFORMATION ON INFORMATION AND COMMUNICATION SYSTEMS (CIS)

Security Accreditation of Communication and Information Systems (CIS)

22. Security accreditation shall be performed for all contractors' CIS that are used to handle (store, process or transmit) NATO RESTRICTED (NR) information.

23. This contract security clause contains the rules and regulations that shall be applied by the contractor's SO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the contractor as a result of the contract. This clause includes specific provisions to be satisfied by the contractor under delegation from the Contracting Authority for the accreditation of the contractor's CIS handling NR information. Under this delegated authority the contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the contractor's response in acknowledgement of the receipt and requirements of the Security Aspects Letter associated with the contract.

24. It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

25. The SO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

26. The following describes the minimum security requirements for handling NR information on contractors' CIS that shall be met:

26.1 Identification and Authentication

26.1.1. An up-to-date list of authorised users shall be maintained by security management staff.

26.1.2. Credentials shall be established and maintained to identify authorised users.

26.1.3. Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.

26.1.4. Passwords shall be a minimum of 9 characters long and shall include numeric and “special” characters (if permitted by the system) as well as alphabetic characters;

26.1.5. Passwords shall be changed at least every 180 days. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.

26.1.6. The re-use of a number of previous passwords shall be denied.

26.1.7. The system shall provide only limited feedback information to the user during the authentication process.

26.1.8. Accounts that are no longer required shall be locked or deleted.

26.1.9. When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

26.2 Access Control

26.2.1. The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security-related documentation.

26.2.2. From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.

26.2.3. Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.

26.2.4. Access to security and system information shall be restricted to only authorised security and system administrators.

26.2.5. Access privileges shall be implemented to restrict the type of access that a user may be permitted (e.g., read, write, modify, and delete).

26.2.6. The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.

26.2.7. The system shall allow user-initiated locking of the user’s own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.

26.2.8. Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

26.3 Security Audit

26.3.1. An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:
- all log on attempts whether successful or failed;
- log off (including time out where applicable);
- the creation, deletion or alteration of access rights and privileges;
- the creation, deletion or alteration of passwords.

26.3.2. The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in humanreadable format either directly (e.g., storing the audit trail in human-readable format) or indirectly (e.g., using audit reduction tools) or both.

26.3.3. Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.

26.3.4. The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.

26.3.5. A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security violation).

26.4 Protection against Malicious Software

26.4.1. Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependant upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).

26.4.2. The virus/malicious code detection software shall be regularly updated.

26.5 Mobile Code

26.5.1. The source of the mobile code shall be appropriately verified.

26.5.2. The integrity of the mobile code shall be appropriately verified.

26.5.3. All mobile code shall be verified as being free from malicious software.

26.5.4. Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

26.6 Availability

26.6.1. Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

26.7 Import/Export of Data

26.7.1. Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.

26.7.2. All data imported to or exported from the CIS shall be checked for malware.

26.8 Configuration Management

26.8.1. A detailed hardware and software configuration control system shall be available and regularly maintained.

26.8.2. Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.

26.8.3. Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.

26.8.4. An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.

26.8.5. The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.

26.8.6. The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects i.e. any potential adverse affects of the modification on existing security measures, shall be considered and appropriate action taken.

26.8.7. The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.

26.8.8. The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.

26.8.9. Changes to the system or network configuration shall be assessed for their security implications/impacts.

26.8.10. The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

26.9 Security Management

26.9.1. Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.

26.9.2. The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

26.10 Approved products

26.10.1. An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

26.10.2. The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

26.11 Security Testing

26.11.1. The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

26.12 Transmission Security

26.12.1. NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using approved cryptographic products.

26.13 Wireless LAN

26.13.1. The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

26.13.2. NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

26.14 Virtualisation

26.14.1. When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

26.14.2. A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

26.14.3. Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

26.14.4. Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure. For example, a firewall shall not be virtualised.

26.14.5. The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

26.14.6. Access to the hypervisor functions shall be appropriately controlled.

26.14.7. The ability to “cut-and-paste” between virtual machines shall be appropriately configured and controlled.

26.14.8. The ability to create virtual machines shall be appropriately configured and controlled.

26.14.9. Virtual Machines shall be suitably de-commissioned after use.

26.14.10. Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

26.14.11. Virtual Servers and Virtual Workstations shall not be located on the same physical host.

26.14.12. Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be located on the same physical host as those operating in the LAN.

26.14.13. The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti malware and Active Directory communication mode shall be allowed.

26.14.14. Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative account.

26.14.15. The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.

26.14.16. The SAN used to host Virtualisation operating at different security classifications shall be isolated onto separate Logical Unit Numbers.

26.14.17. Modifications to the ‘Master Copy/Version’ of a Virtual Machine shall be appropriately controlled.

26.14.18. Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

26.15 Interconnections to a CIS not accredited to handle NR information

26.15.1. Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled “INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)” (current reference AC/322-D/0030-REV5) and “Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet” (current reference AC/322-D(2010)0058). These Directives may be obtained from the Contracting Authority.

26.15.2. Interconnection to another CIS, especially the internet, will significantly increase the threat to a contractor’s CIS and therefore the risk to the security of the NR information handled by the contractor’s CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process. Security requirements can also be found in the latest version of the NATO document entitled “INFOSEC Technical & Implementation Directive for Computer and Local Area Network (LAN) Security” (current reference AC/322-D/0048-REV2). This Directive may be obtained from the Contracting Authority.

26.15.3. When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

26.16 Disposal of IT Storage Media

26.16.1. For IT storage media that has at any time held NR information the following sanitization shall be performed to the entire storage media prior to disposal:
- EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives): overwrite with random data at least three times, then verify storage content matches the random data;
- Magnetic Media (e.g. hard disks): overwrite or degauss;
- Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of $10mm^2$ or less;
- Other storage media: seek security requirements from the Security Accreditation Authority.

26.17 Portable Computing Devices (laptops, tablets, etc)

26.17.1. Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR information that do not use approved encryption shall not be taken outside the contractor's premises unless held under personal custody. The term "drives" includes all removable media. Any authentication token and/or password(s) associated with the encryption product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

Physical Security of CIS Handling NR information

27. Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

28. CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

Security of NR Removable Computer Storage Media

29. Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle.

Use of CIS Equipment Privately Owned by Contractor's Personnel

30. The use of privately-owned equipment of contractor's personnel (hardware and software) for processing NR information shall not be permitted.

CIS Users' responsibilities

31. CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The

responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

Advice

32. Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

Audit/inspection

33. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor shall provide evidence of compliance with this Contract Security Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.