PS26

JNCC Computer Virus Policy

April 2004

1   JNCC Computer Virus Policy

"The JNCC and its support unit staff will undertake all possible measures to reduce the effects and spread of computer software viruses"

2   Contractor Requirements

2.1   The contractor should note that: The supply of computer viruses to the JNCC will prejudice the success of obtaining future contracts, unless the contractor can demonstrate adequate precautions against infection and transmission were taken.

2.2   The contractor **must** bring the contents of this Annex V and JNCC anti-virus policy to the attention of any sub-contractors.

2.3   The contractor **must** accept responsibility for viruses introduced by any sub-contractor.

2.4   Introduction of a virus into the JNCC by the contractor, or their representative, makes the contractor liable for costs of 10% of the value of the contract or the actual cost of the cleanup operation, whichever is greater.

2.5   The contractor **must** provide details of the computer virus detection and virus eradication software (or hardware) used by the contractor to prevent infection of hardware, to the JNCC nominated officer. The contractor **must** state the source of the software, the frequency with which it is updated and that they are licensed to use it.

2.6   If the contractor has no means of detecting or eradicating a virus then a statement to this effect **must** be made.

2.7   The contractor **must** provide details of the actions that are undertaken when a computer virus is detected on the contractor's own site.

3   Contractor working on JNCC premises

3.1   Before using any software on JNCC equipment, the contractor **must** virus check any portable media brought in with the contractor, with the virus checking software provided by the JNCC.

3.2   Before commencing work at a JNCC site the contractor **must** acquaint themselves with JNCC anti-virus policy and JNCC anti-virus software and its use.

4   Contractor sending media to the JNCC

4.1   Media of any type or format supplied to the JNCC by the contractor **must** be checked for viruses before shipment.

4.2   The contractor **must** provide printed and dated output to show that the media was virus free immediately prior to leaving the contractors premises. In the case of tapes or backups the contractor **must** provide proof that the source was virus free immediately prior to the creation of tape or backup.

5   **Bringing Portables onto JNCC premises**

5.1   A contractor **must** not, under any circumstances, connect or attempt to connect a portable computer of any sort, to any of the JNCC's Local Area Networks without the IS Team's, or their appointed representative's, approval. The contractor or their representative **must** have demonstrated that the machine is free from viruses before approval will be given, JNCC's own virus scanning software may be used for this purpose.

5.2   The contractor **must** not transfer files, either via floppy, USB memory stick or other means, from a portable to a machine connected to any of the JNCC Local Area Networks without having first demonstrated that, both the machine and the media being used to transfer files, are free from viruses.

6   **Sending emails to the JNCC**

6.1   Although JNCC is capable of receiving information electronically via email, the contractor will not send email files greater than 10Mb in size. Care should be taken not to send .exe, bat, vbs or macro files. If these types of electronic files are being sent, the contractor will zip these files up using some zipping technology and then send them as an email attachment.

6.2   Every effort should be made to ensure that emails sent should be virus free before leaving the contractors email system. If deliverables of the contact include email exchange between the JNCC and the contractor, JNCC will require details from the contractor of either the anti virus software used or any third party provider used to ensure that all emails are virus free.