APPENDIX B
(TO THE GENERAL TERMS & CONDITIONS FOR IT CONTRACTS)

DECLARATION

AND CONDITIONS OF USE

REGARDING ACCESS TO EMSA'S INFORMATION SYSTEMS

The undersigned,

[forename, surname, function]

representing

[*full official name of the economic operator*]
[*official legal form*]
[*statutory registration number or ID or passport number*]
[*full official address*]
[*VAT registration number*]

(hereinafter referred to as "the contractor")

declares that the contractor will comply with the security and confidentiality rules laid down in the FWC and in particular with the present conditions of use regarding access to EMSA's information systems.

CONFIDENTIALITY

The contractor will strictly comply with the provisions on confidentiality set out in Art. II.8 of the FWC. Without prejudice to the application of Art. II.8.1 FWC, "confidential information" shall also mean all information or documents disclosed to an employee/agent of the contractor or obtained by him in conjunction with the implementation of the FWC the nature of which is such that the employee/agent can reasonably be expected to consider it to have a political, economic or security related importance or to be otherwise of a sensitive nature, even if it has not been explicitly so identified.

In case confidential information has to be disclosed by the contractor under Art. II.8.3(c) FWC, the contractor shall immediately notify EMSA thereof in order to allow its intervention.

At the request of EMSA the contractor shall immediately return the confidential information, both originals and copies, or, if requested, destroy or delete them.

The contractor will strictly comply with Art. I.17 FWC and is aware of the fact that, in case of non-compliance, it may get denied, without prior notice or justification, further access to EMSA premises, information or information systems.

ACCESS TO EMSA INFORMATION SYSTEMS

The employees and/or agents of the contractor shall:

– not access services for which they have not been explicitly granted authorisation, whether or not the services in question belong to the Agency;
– not disclose authentication procedures or share them with third parties unless required to do so by the needs of the performance of the FWC; authorised users shall be responsible for action taken in their name; any action constituting a breach of security may be recorded;
– not install or use on computers supplied by the Agency for the implementation of the FWC (work stations, local or central servers, etc.) any equipment or programs developed outside the Agency, whether free of charge or not, from portable storage media or downloaded from external repositories, unless as part of the performance of the FWC;
– not install connections on computers supplied by the Agency with networks outside the Agency without explicit authorisation;
– notify the Project Officer and the security staff of the Agency as soon as they spot any failure or incident or vulnerability affecting the Agency's information systems;
– not investigate the security of the information systems themselves, unless authorised and supervised by the Project Officer and the security staff of the Agency.

REMOTE ACCESS

The contractor might be granted remote access to EMSA IT Systems on a per-project/per-need basis, on EMSA's sole decision. The current model for remote access follows the following process:

1) EMSA authorises remote access for the contractor to specific IT systems on a strict per-need basis;
2) The contractor connects via Virtual Private Network (VPN) to the EMSA Security Gateway;
3) The EMSA Security Gateway will only allow the contractor to execute a remote desktop session from his PC to a working console hosted at EMSA and dedicated specifically to the contractor and to its project;
4) From the working console hosted at EMSA, the contractor will have access rights strictly limited to the environments relevant to the project, normally a test environment only and related development services.

Specific remote access technologies, and the remote access model itself, might evolve over time following the evolution of IT security and systems at EMSA. The contractor should inquire about the specific technologies and access model details at the time of implementation of the contract, and be able to comply with it in terms of installation of the required software (i.e. VPN client, certificates, tokens for two factor authentication etc.) and in terms of security requirements (i.e. antivirus or patches might have to be installed on the client connecting via VPN to EMSA, and only specific versions of Windows client might be able to connect).

When the specific remote access technologies, and the remote access model itself, will be changed during the execution of the contract following the evolution of IT security and systems at EMSA, the contractor will receive via email the implementing details of the new model and technologies. The contractor has to comply with it within 1 month and must confirm its compliance by answering to the email.

COMPLIANCE WITH THE PRESENT CONDITIONS OF USE

The contractor shall pass these conditions of use or a copy of them to:

    (a) its personnel involved in the implementation of the FWC;

    (b) any natural person with the power to represent the contractor or take decisions on its behalf and which

        is involved in the implementation of the FWC;

    (c) third parties involved in the implementation of the FWC, including subcontractors.

The contractor shall ensure that the persons referred to above have read, understood and fully acknowledged these conditions of use.

The contractor acknowledges that compliance with these conditions of use and with the legal and contractual provisions referred to therein is mandatory and that non-compliance may trigger contractual sanctions, liability in accordance with applicable national and EU law and/or legal action under national law.

Place and date:

Signature: