CONDITIONS OF USE
REMOTE ACCESS TO EMSA IT NETWORK

EMSA provides remote access to its IT systems to selected contractors in order to facilitate the performance of services. Contractors are required to accept and observe the current Conditions of Use in order to ensure the EMSA IT systems are not compromised in the course of using the remote access facility.

1. **Physical and logical protection measures of the Contractor**
As defined in its ICT Security Policy in Annex II of this agreement, the Contractor protects its IT network and sub-networks from which remote access to the EMSA IT network is performed efficiently against intrusion, malware, malicious code and other threats. All tasks are carried out in a physically protected environment with logically protected information technology equipment, which EMSA representatives may inspect at request.
The Contractor's network is connected to any other network through a firewall corresponding to the latest industry standards.
The Contractor implements strictly its IT Security Policy which has been submitted to EMSA. Any changes to this policy and any incident that calls the efficiency of its security policy in question shall be reported with no delay to EMSA.
The Contractor performs the remote access to EMSA's VPN through professional Personal Computers specially designated for that purpose, and not through any other private or public Personal Computer.
These Personal Computers operate at all time during the use of the remote access facility with an operating system compatible with the EMSA VPN client software with the latest security patches, are configured with industry standard anti-virus software using the latest anti-virus signatures files and are malware free when scanned by the EMSA VPN anti-malware scanner.

2. **Connecting to EMSA network**
The Contractor's specifically designated staff and other collaborators access EMSA networks solely from the Contractor's network. The Contractor ensures that remote access will not be implemented from any other network or stand-alone host by introducing adequate measures, including an adequate physical control and protection of the physical protection devices (tokens) that are provided by EMSA.
The Contractor maintains a register of designated authorised staff and other collaborators and provides a list of such to EMSA. Any changes to the list of designated authorised staff and other collaborators shall be communicated to EMSA.
The Contractor informs the designated authorised staff and other collaborators about these Conditions of Use and requires an undertaking in writing by the designated authorised staff and other collaborators to comply with the rules and standards in place at any time when accessing EMSA IT networks under the remote access arrangements. Any failure to accept such undertaking in writing shall lead to the exclusion of the staff and other collaborators from the project carried out under the service contract.
The Contractor ensures that the software and hardware measures and mechanisms to ensure identification and authentication of any remote access defined and provided by EMSA are properly installed and used in compliance with this agreement and solely for the purposes of the contractual tasks defined in this agreement and the service contract.
The Contractor is responsible for the internal management and assignment of the authentication and identification mechanism(s) to its designated authorised staff and other collaborators.
The Contractor is liable for the consequences of the misuse or loss of the authentication and identification mechanism(s) allowing the use of EMSA systems by persons not belonging to the designated authorised staff and other collaborators.

3. **Specific duties of the Contractor**
The Contractor undertakes:
- to use the resources provided by EMSA for no other purpose than to execute the tasks for which they are provided;

- to destroy all data, which he has transferred to his premises or other data storage facility under his control in order to perform the tasks defined by this agreement once they are no longer needed for the tasks required by EMSA,
- not to put out of service the mechanisms set up in the course of this agreement,
- to apply best efforts to remedy as soon as possible any fault, problem, weakness that could appear and for which he is responsible, including those not foreseen in the course of this agreement and inform the EMSA IT Security Coordinator of any such incidences,
- not to disclose to any third party or any member of staff unless on a strict need-to-know basis and technical information or data that may facilitate unlawful or malicious intrusion into EMSA networks. Such information shall be kept under strict physical control (safe) and shall be protected against undetected copying.

4. Designated authorised staff and other collaborators

Members of the designated authorised staff and other collaborators:
- conform to the security rules and policies of the Contractor;
- do not disclose any information held by the Contractor on behalf of EMSA to third parties, except on a need-to-know basis where authorised;
- make use of all reasonable means of controlling access provided by the Contractor and in balance with the sensitivity of the information system concerned to prevent unauthorised persons from using the resources at their disposal, in particular by ensuring that computer terminals are not accessible during absences, however short these absences may be;
- do not access services for which they have not been explicitly granted authorisation, whether or not the services in question belong to the Contractor or to EMSA;
- do not disclose authentication procedures or share them with third parties unless strictly required to do so by the needs of the service and following consultation of the EMSA IT Security Coordinator;
- do not install or use on computers (work stations, local or central servers, etc.) any equipment or programmes, from portable storage media (diskettes, optical disks, etc.) or downloaded from electronic bulletin boards, e-mail systems or telecommunications networks belonging to third parties, unless explicitly authorised by the Contractor;
- do not install or have installed connections with networks without explicit authorisation from the Contractor;
- do not set up electronic bulletin boards, e mail systems, modem connections or any other type of information communication system that could enable unauthorised persons gaining access to the Contractor's or EMSA's systems;
- do not use equipment or software that is their private property when connected to the Contractor's and/or EMSA's network without prior explicit authorisation from the Contractor;
- notify their superior as soon as they suspect any failure or incident affecting the security of their own IT Network environment or of other systems;
- take all possible steps in respect of availability, confidentiality and integrity to safeguard the security of their working environment, particularly as regards working methods they have introduced or developed themselves.

5. Obligations

The contractor and EMSA undertake:
- to inform each other of any attack on the security mechanisms of their systems that could affect the security of the other;
- not to hold each other liable for delays occasioned by shutdowns of their systems in order to enforce security or repair damage caused by attacks from a third party whether known or unknown;
- to act immediately to cease data communication with the other if in good faith they believe that the security of either of the networks for which they are responsible is at risk and until that risk is identified and countered.

6. EMSA remote access environment

An authentication mechanism and an access control mechanism managed by EMSA are set up at the connection point with EMSA's internal network. These mechanisms ensure that only the designated authorised staff and other collaborators of the Contractor have access to EMSA's internal resources when it is granted to perform contractual tasks. EMSA staff is able to interrupt remote interventions immediately and at any time from its premises. The remote intervention process grants only the access rights assigned by EMSA staff from their premises. An audit trail is generated in the EMSA environment.

7. Authentication and identification

At the boundary of EMSA's network, the mechanism for authentication and identification is based on a two factors authentication using credentials (username + password) plus a one-time-password which is currently provided by a hardware RSA token. EMSA reserves the right to change schema and technologies involved in the authentication process at any time, informing in advance the Contractor. The one-time-password device will be sent to the representative of the Contractor. The associated credentials will only be sent after reception (by means of a fax) of the acknowledgement of reception for the token(s). This document with acknowledgement of receipt must be signed by a duly authorised representative of the Contractor. When a member of the designated authorised staff and other collaborators wants to connect to an EMSA ICT resource (inbound connection), a VPN tunnel shall be initiated establishing a session with the VPN gateway of EMSA. The VPN gateway sends back an authentication request. This request must be answered by sending the credentials together with the value shown on the one-time-password device. If the authentication is successful, the connection to the EMSA resource is open. The tokens are under the sole responsibility of the Contractor.

The establishment of the VPN tunnel imposes the usage of a specific VPN client. Currently EMSA delivers client software for Microsoft Windows only - that the Contractor is required to use. Access by other means such as third party clients or web based clients, is explicitly forbidden. The VPN client software launches a security compliance checking during the VPN tunnel establishment. The windows machine is required to have the latest service pack and security patches installed and an updated anti-virus with on-access scanner capabilities. A quick audit of the client machine is also performed searching for traces of malware. If the windows client machine is found to be non-compliant, the remote access to EMSA is denied.

All costs linked to the remote access to the EMSA network, like telephone costs, costs of leased line, costs of routers and costs of spare hardware VPN client must be borne by the Contractor.

8. Access & Contact Grids

In Appendix 1 of this agreement are detailed the following:

1. Contractor's contacts for remote access setup and incident handling;
2. Contractor's staff for which remote access tokens are requested;
3. EMSA Contacts for remote access setup and general project and ICT security incident handling;
4. To which EMSA applications and information assets the contractor will be granted access;
5. Relevant contractor's data transmission network details.

Accepted:

For the Contractor