GSA/OP/09/14

"General ICT Support"

ANNEX I.L to the Tender Specifications
Draft of the Security Convention for Remote Access to GSA Information Systems

Security Convention for Remote Access to GSA Information Systems based the FWC GSA/OP/09/14

Between the European GNSS Agency, represented for the purposes of the agreement by

……. for the GSA

Hereinafter called "the Agency", of the one part,

and

Name of Company

Whose registered office is at:

Address

represented for the purposes of the agreement by

Name and role

Hereinafter called "the Contractor", of the other part,

It is agreed as follows:

I. Objective

The objective of this document is to define the rules applicable to remote access to the internal information technology resources of the Agency from the Contractor's IT systems.

II. Purpose

The remote access is granted solely for the execution of tasks defined in valid Specific contracts under the FWC GSA/OP/09/14 and only for the time periods defined in the Specific contracts.

III. Technology and equipment

1. The GSA technology available for the remote access is the following:
   a) VPN over Internet utilising Secure Socket Tunnelling Protocol (SSTP)
   b) Utilising GSA supplied SSL certificates, usernames and passwords for identification and authentication of authorized users
2. The Contractor's equipment ("workstation") allowed for the remote access is the following:
   a) A standalone laptop, desktop, server, tablet or smartphone
   b) A laptop, desktop or server connected to Contractor's network for the purpose of Internet access

IV. Rules

In order to perform the remote access, the Contractor must comply with the rules defined below. Failure to comply with those rules will result in the revocation by the Agency of the credentials needed for the remote access. In this case, the Agency will consider the Contractor responsible for the operational problems caused by his unreadiness to connect.

V. Authorised Staff

1. The Contractor shall ensure that the remote access is requested only by authorised staff, i.e. staff specifically designated for the execution of tasks described in Specific contracts.
2. The Contractor must create and maintain a register of the members of the authorised staff (Annex I) and send an update to the GSA upon every change.
3. Each member of the authorized staff must submit to the Agency a request for remote access using the form in Annex II; the form should be submitted via the Contract manager.
4. The GSA may require completion and/or clarifications of the information in the form and has the right to decide whether the remote access will be granted or not.
5. VPN certificates and passwords MUST NOT be sent by email and must be handed over in a reasonably secure way. Should there be any doubt about the possibility that they have been compromised, they must be immediately revoked and replaced with new ones.
6. Authorised staff shall not disclose information held by the Contractor on behalf of the Agency to third parties, except on a need-to know basis where authorised.
7. Authorised staff shall 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 they may be.
8. Authorised staff shall 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 the Agency.

9. Authorised staff shall not disclose authentication procedures or share them with third parties unless required to do so by the needs of the service;
10. Authorised staff shall be responsible for action taken in their name.
11. Authorised staff shall not install or use on the workstations any equipment or programmes, from portable storage media or downloaded from the internet belonging to third parties, unless explicitly authorised by the Contractor.
12. Authorised staff shall not install or have installed connections with networks without explicit authorisation from the Contractor.
13. Authorised staff shall not set up any type of information communication system that could enable unauthorised persons to gain access to the Contractor's or Agencies systems.
14. Authorised staff shall not use equipment or software that is their private property when connected to the Contractor's and / or Agencies network without prior explicit authorisation from the Contractor.
15. Authorised staff shall notify their superior in the Contractor as soon as they suspect any failure or incident affecting the security of their own environment or of other systems.
16. Authorised staff shall 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.
17. Authorised staff shall not share their certificates or login credentials with any other person.
18. Authorised staff will only activate the VPN connection with the Agency when the need arises according to the tasks assigned to the individual and will deactivate the connection immediately after the remote intervention is completed; a permanent connection is not permitted.
19. Immediately before each activation of a remote connection the Authorised staff must notify by e-mail the GSA helpdesk and provide the following information:
    - Purpose of the remote intervention
    - Systems to be accessed during the intervention
    - Expected duration of the intervention
    - Phone number on which he/she is accessible during the intervention

    This e-mail will be used for tracking purposes and does not have to be answered by the GSA.
20. Immediately after the termination of a remote connection the Authorised staff must notify by e-mail the GSA helpdesk and provide the following information:
    - Result of the remote intervention
    - Systems actually accessed during the intervention
    - Whether this intervention is completed or will continue

    This e-mail will be used for tracking purposes and does not have to be answered by the GSA.

VI. Authentication / Identification of the Authorised Staff

1. Each member of the Authorised staff using equipment connected to the Agencies network must be clearly identified and authenticated.

2. The Contractor ensures that the Authentication / Identification mechanism(s) are used in compliance with the conditions of this agreement, and solely for the purposes of the contractual tasks defined in this agreement.
3. The Contractor is legally, jointly and severally liable for the consequences of the misuse or loss of the Authentication / Identification mechanism(s) allowing the use of the Agencies systems by persons not belonging to the Authorised staff.

VII. The Contractor environment

The contractor will ensure that any workstation having remote access to the Agencies facilities will comply with the following:

a) Be provided, hardened and managed by the Contractor (no use of privately owned equipment is permitted)
b) Be protected by either a local or corporate firewall
c) Have the latest operating system patches, no more than 2 weeks since last update
d) Have an up to date antivirus, no more than 1 week since last update
e) Contain no malware
f) Contain no known vulnerabilities that may pose a threat to the Agencies systems
g) Do not share the remote access to the Agency with other systems (Be not configured in a way allowing further routing of network traffic from/to other computers or systems)

VIII. Contractor specific duties

The Contractor undertakes:

a) To use the resources provided by the Agency for no other purpose than to execute the tasks in object.
b) To destroy all data, which he has transferred to their premises in order to perform the tasks defined by this agreement once they are no longer needed for the tasks required by the Agency.
c) Not to put out of service the mechanisms set up in the course of this contract.
d) To best efforts to remedy as soon as he can any fault, problem, weakness that could appear and for which he is responsible, including those not foreseen in the course of this contract.
e) To comply with new security rules at the request of the Agency, for example if the Agency implements new Authentication and Access control mechanisms for the connection to its internal network provided that this does not incur unreasonable expense.
f) TTo collaborate with the Agency at any moment in time on the verification of the compliance of Contractor's workstations with the above requirements for remote access including the facilitation of access of designated GSA staff to the Contractor's premises
g) To collaborate with the Agency on the investigation of security incidents including the provision of security and audit logs from the Contractor's workstations and systems
h) To provide the Agency upon a request with more information about the technical solutions used by the Contractor in order to fulfil their obligations.

IX. Mutual undertaking

Both parties to the agreement undertake:

a) To inform each other of any attack on the security mechanisms of their systems that could affect the security of the other.
b) 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.
c) To act immediately to cease 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.

X. Contact points

The parties agree to use the following contact details:

The Agency:

Purpose	Name	Phone	e-mail
Normal communication within business hours	GSA helpdesk	+420 234766600	helpdesk@gsa.europa.eu
Outside business hours or escalation of issues	GSA Operations Manager	To be filled	To be filled
Security incidents	GSA IT Security Officer	To be filled	To be filled

The Contractor:

Purpose	Name	Phone	e-mail
Normal communication within business hours	To be filled	To be filled	To be filled
Outside business hours or escalation of issues	To be filled	To be filled	To be filled
Security incidents	To be filled	To be filled	To be filled

XI. Final provisions

The provisions of this document may be modified by a written agreement of the parties.

SIGNATURES

For the contractor,	For the European GNSS Agency,
[*Company name/forename/surname/function*]	…….
signature[s]: _____	signature:_____
Done at [place], [date]	Done at Prague, [date]

In duplicate in English.

Annex I – List of authorized staff

Company	Surname	Forename	System Requiring Access	Level of Access	Specific contract	Task	From-To

Annex II: Request for Remote Access to GSA IT Systems

This form must be filled-in by the each member of the Authorised staff and submitted via the Contract manager to the GSA helpdesk. As a response, the GSA will normally provide the person with a VPN certificate, username and password needed for the remote connection.

Important: VPN certificates and passwords MUST NOT be sent by email and must be handed over in a reasonably secure way. Should there be any doubt about the possibility that they have been compromised, they must be immediately revoked and replaced with new ones.

Personal details	
Company	
Surname	
Forename(s)	

Purpose of remote access	
Specific contract (SC)	
Task in the SC	
From-to period according to the SC	
System(s) requiring remote access	
Level of access	

Workstation	
Brand and model	
Serial number	
Inventory number	
MAC address – Ethernet	
MAC address – Wireless	
Operating system	
Frequency of OS patching	
Disk encryption (yes/no, software used)	

Antivirus software	
Frequency of antivirus updates	
Firewall details (yes/no, software used, configuration policy)	
Additional security measures implemented	
Applications and communication protocols used for remote access (names, versions)	

Signature (the above information is true and complete)	
Authorised staff	
I have read and understood the Security Convention for Remote Access to GSA Information Systems.	
Date, signature	
Comments	

Contractor's technical validation of the above information	
Function/role	Name, date, signature
Comments	

Contractor's operational validation (the remote access in needed for the execution of SC)	
Contract manager	Name, date, signature
Comments/Instructions	

GSA operational validation (acknowledge of the need for remote access)	
GSA Operations Manager Visa	Name, date and signature
Comments/Instructions	

GSA security validation (security assessment of the request)	
Decision: Access granted Yes/No	
GSA IT Security Officer Visa	Name, date and signature
Comments/Instructions/Reason for rejection	

Handover of credentials (if access granted)	
Username assigned	
GSA Helpdesk Visa	Name, date and signature
Authorised staff receipt confirmation	Date, signature