EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

SECURITY CONVENTION FOR REMOTE ACCESS.Part2

N°: <dg acronym>.<serial number>.T1[1]

Convention Version N°	

Template version 8.1 Reference number: Ares(2015)2847392–07/07/2015

[1] Security Convention ID is allocated by HR.DS.
Contact: EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu

Between

the European Commission,

represented for the purposes of the agreement by

- Ms Maresa MEISSL for the Security Directorate
- Mr Guy DROWART for the Directorate-General for Informatics
- ***<DG or Service representative(s)>***

Hereinafter called "the Commission",

of the one part,

and

<company name>

whose registered office is at ***<company address>***

represented by ***<name of company representative>***, ***<function of company representative>***,

Hereinafter called "the Contractor",

of the other part,

It is agreed as follows:

Table of Contents

1. PREAMBLE

The provisions of this document may be modified by the agreement of the parties. This document makes part of a set of two documents. A first document « SECURITY CONVENTION FOR REMOTE ACCESS.Part1» describes the contractor's physical and logical protection measures and the contractors sub-network. The information contained in that document could not be added to this present document because of confidentiality of the information.

Version 1 of this document represents the initial convention. Amendments to this first version could be done with the agreement (formal signature) of all the parties by issuing a new version of this entire document. Any amendment will replace any previous version. In the case of the change initiated by DIGIT (e.g. upgrade of database, server migration to the new infrastructure, etc.), the amendment can be performed without the formal signature circuit, as long as it concerns only changes to approved accesses. Such a change can, however, have an impact on the contractor's remote computer platform configurations.

The version of the convention is specified under the reserved frame on the first page of the document.

2. OBJECT

The present document sets up the rules required for the Contractor to perform remote access on the Commission internal information technology resources from Contractor premises. The remote access is permitted in order for him to execute the tasks defined in a specific Framework Contract and its Specific Agreement.

The Annex V gives a reference of the Framework Contract and its Specific Agreement, the end date of the specific agreement, the Contractor address premises and it describes the authorised remote access.

3. 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 interruption by the Commission of the accesses to the resources described in Annex V. In this case, the Commission will consider that the Contractor is responsible for the interruption of service.

3.1. Authorised Staff

(1) The Contractor shall ensure that the tasks entrusted to him and specified by this agreement are carried out only by authorised staff, i.e. staff specifically designated for the purpose.

(2) The Contractor must keep a register of the members of the authorised staff. The Contractor shall grant access to the register on request of the Commission.

(3) The contractor shall instruct the Authorised staff to comply with the security standards and rules set out below and as specified in Annex I.

3.2. Authentication / Identification of the Authorised Staff

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

(2) The Contractor shall install the mechanism(s) delivered by the Commission for this purpose (see Annex II).

(3) 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.

(4) The Contractor is responsible for the internal management and assignment of the Authentication / Identification mechanism(s) for its staff.

(5) 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 Commission systems by persons not belonging to the Authorised staff.

3.3. The Contractor environment

Consult the document «SECURITY CONVENTION FOR REMOTE ACCESS.Part1»

3.4. Contractor specific duties

The contractor undertakes:

(1) To use the resources provided by the Commission for no other purpose than to execute the tasks in object;

(2) To destroy all data, which he has transferred to his premises in order to perform the tasks defined by this agreement once they are no longer needed for the tasks required by the Commission;

(3) Not to put out of service the mechanisms set up in the course of this contract;

(4) To best efforts to remedy as soon as possible any fault, problem or weakness that could appear and for which he is responsible, including those not foreseen in the course of this contract;

(5) To comply with new security rules at the request of the Commission, for example if the Commission implements new Authentication and Access control mechanisms for the connection to its internal network provided that this does not incur unreasonable expense.

3.5. Mutual undertaking

Both parties to the agreement undertake:

(1) To inform each other[2] of any attack on the security mechanisms of their systems that could affect the security of the other;

(2) 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;

(3) 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.

4. COMMISSION ENVIRONMENT

In the course of remote access, the Commission puts in place the following mechanisms.

(1) An authentication mechanism and an access control mechanism managed by the Commission, under the supervision of the Security Directorate of the Commission, are set up at the connection point with the Commission's internal network. These mechanisms ensure that only authorised staff has access to the Commission's internal resources when he is granted to perform his contractual tasks.

(2) Commission staff is able to interrupt remote access immediately and at any time from his premises.

(3) The remote access process grants only the access rights assigned by the Commission staff from their premises.

(4) An audit trail is generated in the Commission's environment.

5. ANNEXES

All annexes form an integral part of this document. The following documents are annexed to this document and can not be modified:

Annex I Rules applicable to the members of the authorised staff
Annex II Authentication / Identification Mechanism
Annex III Description of the incident handling procedure
Annex IV Description of the procedure used to set-up and maintain the connection
Annex V Description of the Authorised Remote Access

[2] Procedure to be used is described in Annex IV

Done in Luxembourg on <dd/mm/yyyy>

Each party acknowledging receipt of its copy

For the Contractor

Name:

Function:

For the Commission

Security Directorate

Name: Maresa MEISSL

Function: Head of Unit HR.DS.5

(e-Signatory in ARES)

Directorate General

Name: <Authorised person>

Function: <IRM/HoU of the business unit>

(e-Signatory in ARES)

Name: Kaili KATMANN

Function: ICT Security Analyst

(e-Signatory in ARES)

Name: < Authorised person >

Function: LISO of DG

(e-Signatory in ARES)

Directorate-General for Informatics

Name: Guy DROWART

Function: Head of Unit DIGIT.C.4

(e-Signatory in ARES)

Postal address to be used to return the signed security convention documents to the Commission:

Postal address:

European Commission

Directorate-General Human Resources and Security

Directorate Security /Informatics Security

Security Conventions (HR.DS.5)

DROSBACH B0/006

12, Rue Guillaume Kroll, L-1882 Luxembourg

Name: K KATMANN

Function: ICT Security Analyst

Email: EC-SECURITY-SECURITY-CONVENTIONS@ec.europa.eu

Telephone: +352 4301 37 410

ANNEX I

RULES APPLICABLE TO THE MEMBERS OF THE AUTHORISED STAFF

Members of the authorised staff shall:

(1) Conform with the security rules, policies of the Contractor;

(2) Not disclose information held by the Contractor on behalf of the Commission to third parties, except on a need-to know basis where authorised;

(3) 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;

(4) 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 Commission;

(5) Not disclose authentication procedures or share them with third parties unless required to do so by the needs of the service;

(6) Be responsible for action taken in their name;

(7) 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;

(8) Not install or have installed connections with networks without explicit authorisation from the Contractor;

(9) Not set up electronic bulletin boards, e-mail systems, modem connections or any other type of information communication system that could enable unauthorised persons to gain access to the Contractor's or Commission's systems;

(10) Not use equipment or software that is their private property when connected to the Contractor's and / or Commission's network without prior explicit authorisation from the Contractor;

(11) 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;

(12) 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.

ANNEX II
AUTHENTICATION / IDENTIFICATION MECHANISM TO ACCESS THE RESOURCES DESCRIBED IN ANNEX V

1. ACCESS TO THE EC NETWORK

At the boundary of the Commission's network, the mechanism is a token provided by the Commission. Each member of the authorised staff receives a token that is under his control.

When a member of the authorised staff wants to connect to a Commission IT resource (inbound connection) as described in Annex V, he initiates a VPN tunnel. A session is established with the VPN gateway of the Commission. The VPN gateway sends back an authentication request. This request must be answered by sending the token identifier together with the value shown on the token's screen. If the authentication is positive, the connection to the Commission resource is open.

The Commission delivers the tokens needed by the contractor. The tokens are under the sole responsibility of the contractor. They are password protected and subject to appropriate security measures.

The establishment of the VPN tunnel imposes the usage of a specific VPN client. If the platform used by the members of the Authorised staff is Microsoft Windows, the Commission delivers the client software. If other platforms are used, the Commission lends a hardware client for the duration of the security convention. The Commission delivers the hardware client already configured. The Contractor may not change the configuration. No maintenance is done ‘on site’ and the hardware client must be returned to the Commission’s premises in case of hardware or software problems. A second hardware client may be bought by the Contractor in order to have a spare part available. The Commission will configure this hardware client.

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

2. RESOURCES AUTHENTICATION / IDENTIFICATION MECHANISM

Specific access control mechanisms are in place for each resource to protect the resource assets against unauthorised access.

Depending of the data handled by the system, different type of identification and authentication can be in place; usually a UserID/Password pair is used but other method such as strong passwords can be necessary.

ANNEX III
DESCRIPTION OF THE INCIDENT HANDLING PROCEDURE

PROCEDURE TO BE USED TO:

Stop security threats:

– inform each other of any attack on the security mechanisms of their systems that could affect the security of the other;

– 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;

Incident handling:

– signal abnormal interruptions of the remote access

Support set-up of the Commission:

Administrative information used (by the contractor) for incident handling

During office hours the contractor must call the IT Infrastructure Consolidation Help Desk (ITIC Help Desk) or Local Help Desk (where applicable).

ITIC Help Desk

Working hours: 08h00 -- 18h00

Name of contact: EC HELPDESK IT

Telephone number: +32 229 77777

E-Mail EC-HELPDESK-IT@ec.europa.eu

or

Local Help Desk[3]

Working hours: <start hour> -- <end hour>

Name of contact: <DG> Local Help desk

Telephone number: …

Central Help Desk (EC SPOC)

Incidents occurred outside office hours can be signalled to the central helpdesk, which is a call-dispatch available 24h/day 7d/7d. The call is recorded and then transmitted to the concerned service, which will intervene within the framework of its operating mode and its contractual obligations. The concerned service will only intervene if the security of the networks is at risk.

Workflow (both actions are mandatory):
(1) First, send an Email to ec-central-helpdesk@ec.europa.eu
(2) Second, Call +32 2 2958181 (24h/24h 7d/7d)
- Press 1 to reach operator outside working hours (18h -> 8h)
- Back-up number (+32) 0498/50.60.11

Important! The E-mail is only taken into account after your phone call, especially outside working hours:
- All information needed to process your request must be supplied via the e-mail
- each e-mail must be clarified by a phone call

Mandatory Information to be supplied when calling for an incident:
- Sec conv ID
- Token ID

[3] Filled out by the Directorate General (where applicable)

Support set-up of the contractor[4]:

<Explain the procedure used by the contractor>

Administrative information used (by the Commission) for incident handling

Company name: ***<company name>***

Contractor's address premises: <***Contractor's address premises***>

During Working Hours: <start hour> -- <end hour>

Normal procedure

Name of contact person (or help desk): ….
Telephone number: …
GSM number: …
Email address: …

Escalation procedure

Name of contact person (or help desk): ….
Telephone number: …
GSM number: …
Email address: …

Outside Working Hours: W.E. and special holidays: <special holidays>

Name of contact person: …
Telephone number: …
GSM number: …
Email address: …

[4] Filled out by the Contractor

ANNEX IV
DESCRIPTION OF THE PROCEDURE USED TO SET-UP AND MAINTAIN THE CONNECTION

PROCEDURE TO BE USED TO:

– Send a hardware VPN client to the contractors project manager;

– Receive (at the end of the contract or when malfunctioning) a hardware VPN client from the contractor;

*The VPN hardware client **(only for non-windows)** will be sent to the representative of the company. The remote connection will stay closed until reception of the acknowledgement of reception for the VPN hardware client. This « acknowledge of reception» template sent together with the VPN hardware client must be signed by the **representative** of the company. This hardware must be returned to the Commission at the end of the contract or when malfunctioning. The Commission can only allocate one VPN hardware client per connection. A second (spare part) hardware client can be bought by the contractor. This will be configured by the Commission network service.*

Administrative information used by the Commission[5]

Contractor: representative of the company

<Company name>

<***Contractor's address premises***>

Name of the representative of the company: …

Function: …

Telephone: …

Email: …

Signature of 'representative of the contractor » :
Used for the VPN-hardware client « receipt acknowledges»

[5] Filled out by the Contractor **ONLY if VPN hardware client is used**

Administrative information used by the Contractor[6]

Commission: Corporate Infrastructure Services

Contact to return:

- The «receipt acknowledge» message when receiving a VPN hardware client[7]

- A VPN hardware client

Postal address:

European Commission

Directorate-General for Informatics

User Access Administration (UAA)

Office DRB D2/047A

12, rue Guillaume Kroll

L-1882 Luxembourg

Telephone: +352 4301 35035

Email: DIGIT-USER-ACCESS@ec.europa.eu

[6] Filled out by the Commission

[7] The hardware client will be activated only after receiving the 'receipt acknowledges'

PROCEDURE TO BE USED TO:

– Send the TOKEN devices and pin-code to the representative of the company.

– Receive (at the end of the contract or when malfunctioning) the TOKEN devices from the contractor.

*The TOKEN devices will be sent to the representative of the company. The associated pin-code will only be sent after reception of the acknowledgement of reception for the Token(s). This «acknowledge of reception» document sent together with the TOKEN must be signed by the **representative** of the company.*

Administrative information used by the Commission[8]

Contractor: representative of the company

<Company name>

<***Contractor's address premises***>

Name of the representative of the company: …

Function: …

Telephone: …

Email: …

[8] Filled out by the Contractor

Administrative information used by the Contractor

Commission: User Access Administration

Contact to return:

- The « receipt acknowledge » message when receiving a TOKEN device

- The TOKEN device

Postal address:

European Commission

Directorate-General for Informatics

User Access Administration (UAA)

Office DRB D2/047A

12, rue Guillaume Kroll

L-1882 Luxembourg

Telephone: +352 4301 35035

Email: DIGIT-USER-ACCESS@ec.europa.eu

ANNEX V
DESCRIPTION OF THE AUTHORISED REMOTE ACCESS

In execution of ***the Framework Contract or the specific contract and the Specific Agreement(s) listed in the table below***, the contractor, **<*Company name*>,** is allowed to perform the remote access described hereafter until <***End date of ALL the Specific Agreement(s)***> from <***Contractor's address premises – Please specify here the address for each location described in Part 1 of the Security Convention***>. Access to specific resources related with more than one specific agreement will be possible until the latest end date of these specific agreements.

Table 0: Contractual framework between the external company and the Commission		
Framework/Specific Contract (FC/SC)	**Task description[9]**	**End Date**
< Contract N° >	**….**	**….**

9 Give a brief description of the tasks achieved

Table 1: Inbound Network Access to Commission's IT Resources[10]								
ID	**Application** (and DC Rfc number if applicable)	**Component** (Oracle/WebLogic/ColdFusion/Unix account, etc.)	**IP Address AND NAME**[11] (Name or DNS Name or Generic service)	**Location** (DMZ or Data Centre or DG Intranet)	**Service Port**[12]	**Port Description** [13]	**Contract**	**Latest End Date**
1								
2								
3								
…								
10								

[10] For each resource, indicate the services required to perform the tasks described in the specific agreement. Use one line per service even if several services are hosted on the same server.

[11] If the service must be accessed by its URL (e.g. access via reverse proxy), the local hosts file must be populated as the client is not allowed to query EC internal DNS servers. In this case add the following note in the column **IP address and Name** " Note: Configure the hosts file and use the name instead of IP in the URL when using the token"

[12] Application port number (ex: TCP 80, TCP 443, TCP 2010 ...). UDP based applications protocols are not permitted.

[13] Application (protocol) name (ex: HTTT, HTTPS ...). For custom protocols, enter the name of the protocol (if exist) or the name or the application accessed through this protocol (ex: CCN/CSI, COMEXT-CLIENT).

Table 2: Description of Inbound Connections to Commission's IT Resources			
ID	**Description** (What instance/module of the application/service is accessed and which environment: production/training/acceptance/test/development/maintenance)	**Protocols**	**Justification/Reason of request** (For what purpose the access is used by the contractor)
1			
2			
3			
…			
10			

Table 3: Resources Authentication/Identification Mechanism on resource level (application/service/etc) [14]			
ID	**Identification / Authentication mechanism**	**Access Type**	**The System Owner (or Service Provider) who has the right to grant accesses for a specific resource**
1			
2			
3			
…			
10			

[14] Implemented on the server that is accessed via the Commission's central secure access point. For each resource (service), describe the identification / authentication mechanism of the member of the Authorised Staff and the type of access, i.e. read or update. If a document describing the security policy of the accessed resources exists, it can be referenced here. A separate action must be taken by the DG project manager for the creation of login on those servers.

Table 4: Outbound Connections to Contractor's IT Resources[15]					
Resource Description			**Service Description**		
ID	**Source IP Address** (Commission's IT Resource)	**Destination IP Address[16]** (Contractor IT Resource)	**Service Port[17]**	**Port Description[18]**	**Specific agreement(s)**
1					
2					
3					
…					
10					

15 Outbound connections may be authorised when the Data Transmission Network is leased line after consultation of feasibility with the service provider.

16 Access towards the contractor's IT resource will be done via 2 specific IP ranges that will be communicated during the implementation phase of the security convcention.

17 Application port number (ex: TCP 80, TCP 443, TCP 2010 ...). UDP based applications protocols are not permitted.

18 Application (protocol) name (ex: HTTT, HTTPS ...). For custom protocols, enter the name of the protocol (if exist) or the name or the application accessed through this protocol (ex: CCN/CSI, COMEXT-CLIENT).

Table 5: Data Transmission Network used for the Access to the Commission´s IT Resources			
		Inbound Traffic ("P" for primary connection and "B" for back-up connection)	**Outbound Traffic** ("P" for primary connection and "B" for back-up connection)
Type	**Internet**		
	Other: <Please specify the type of Data Transmission Network when different from Internet>		

Table 6: Platform used by the Contractor´s authorised Staff to initiate the connections to the Commission's IT resources[19]			
			Indicate the choice (Put an X, multiple Operating platforms are permitted when Software Client used)
Type[20]	**Software VPN Client**	**Operating platform[21]**	
		Windows 7 x86 (32-bit) and x64 (64-bit)	
		Windows 8 and 8.1 x86 (32-bit) and x64 (64-bit)	
	Hardware VPN Client		

19 Simultaneous access to contractor IT resources and Commission IT resources (mentioned in the table below) is not permitted (i.e. split-tunnlling disabled).

20 Choose EITHER Software VPN Client (for Windows OS platform) OR Hardware VPN Client (other OS platforms/versions), to use both at the same time is not permitted.

21 Support is given ONLY for Windows 7 x86(32-bit) and x64(64-bit) and Windows 8 and 8.1 x86 (32-bit) and x64 (64-bit).