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

SECURITY CONVENTION FOR REMOTE ACCESS. Part1

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

DS Internal use, do not fill

Version N°	
Date of Approval	
Approved by	
Signature	

[1] DG only fills DG acronym, serial number is assigned by HR.DS

Between

the European Commission,

represented for the purposes of the agreement by

Mr. Guido VERVAET for the Security Directorate

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 4

2. OBJECT 4

3. THE CONTRACTOR ENVIRONMENT 4

4. CONTRACTOR SPECIFIC DUTIES 4

5. CONFIDENTIALITY AGREEMENT 5

6. ANNEXES 5

ANNEXE I DESCRIPTION OF THE CONTRACTOR'S PHYSICAL AND LOGICAL PROTECTION MEASURES OF THE WORKING ENVIRONMENT 7

ANNEXE II CONTRACTOR'S NETWORK DESCRIPTION 8

1. ARCHITECTURE / TOPOLOGY 8

2. PERIPHERAL SECURITY INFRASTRUCTURE 8

2.1. Hardware components 8

2.2. Software components 8

2.3. Filtering Rules 8

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 second document « SECURITY CONVENTION FOR REMOTE ACCESS.Part2» describes the set up of the rules required for the Contractor to perform remote access on the Commission internal information technology resources from Contractor premises.

2. OBJECT

The present document describes the contractor's physical and logical protection measures and the contractor's network. The contractor's security policy is an important element that must be taken into account and that must be checked on against our own security policy.

3. THE CONTRACTOR ENVIRONMENT

(1) All tasks must be carried out in a physically protected environment with logically protected information technology equipment, which the Commission may inspect on request. The Contractor must describe, in Annex I, the physical and logical measures put in place.

(2) The Contractor's network must be connected to any other network through a firewall. The Security Directorate of the Commission must approve the security policy implemented on the firewall. The Security Directorate of the Commission must approve any changes to these rules. For other changes, the Contractor must inform the Security Directorate of the Commission. The Contractor must describe, in Annex II, his network architecture as well as the means that are put in place to connect to external networks.

In case of multiple locations, Annexe I and II shall be completed for each location.

Complementary guidelines for the description of the security measures can be consulted in the document "Guidelines for the preparation of SECURITY CONVENTION FOR REMOTE ACCESS.Part 1".

4. CONTRACTOR SPECIFIC DUTIES

The contractor undertakes not to change the elements described in Annexes I and II without prior approval of the Commission.

5. CONFIDENTIALITY AGREEMENT

The information provided by the company to the Commission will only be accessible by authorised staff of the Security Directorate who has the need to know. The information will be handled safely and archived in a safe.

6. ANNEXES

The following annexes form an integral part of the current document:

Annex I: Description of the Contractor's physical and logical protection measures of the working environment

Annex II: Contractor's Network Description

Done at Luxembourg at <date>

Each party acknowledging receipt of its copy

For the Contractor

Name:

Title:

For the Commission

Security Directorate

Name: Guido VERVAET

Title: Head of Unit HR.DS

Name: Kaili KATMANN

Title: ICT Security Analyst

ANNEXE I
DESCRIPTION OF THE CONTRACTOR'S PHYSICAL AND LOGICAL PROTECTION MEASURES OF THE WORKING ENVIRONMENT

The information provided hereafter will be accessible only to authorised staff of the Security Directorate. The documents will be archived safely and only accessible to authorised staff of the Security Directorate.

Please indicate clearly the address of the location. In case of multiple locations, Annexe I shall be completed for each location.

1. PHYSICAL PROTECTION MEASURES

Describe the necessary security measures in place assuring the physical protection of the locations and resources from which the remote access to the Commission's resources is possible. The description should cover following topics (for the further details please consult the corresponding guidelines):

<General description of the location: location of the office(s) in the building, access/entry points (doors, windows)>

<Access controls implemented at access/entry points>

<Access control measures (inside/outside working hours) >

<Protection measures when the areas are left unattended>

2. LOGICAL PROTECTION MEASURES

Describe the necessary security measures in place assuring the logical protection of the resources from which the remote access to the Commission's resources is possible. The description should cover following topics (for the further details please consult the corresponding guidelines):

<Identification/Authentication policies and mechanisms enforced on the devices giving access to Commission's resources>

<Access control mechanism>

<Operating system lock-down (i.e. hardening) and update policies>

<Measures against malicious code and anti-virus/spyware software update policy)>

ANNEXE II
CONTRACTOR'S NETWORK DESCRIPTION

The information provided hereafter will be accessible only to authorised staff of the Security Directorate. The documents will be archived safely and only accessible to authorised staff of the Security Directorate.

In case of multiple locations, Annexe II shall be completed for each location. The description should cover following topics in §1-2 below (for the further details please consult the corresponding guidelines).

1. ARCHITECTURE / TOPOLOGY

<Schema of the network topology providing relevant details of the sub-network to which the workstations of the authorised staff are connected, and of the connection of this sub-network to the Contractor's global network>

2. PERIPHERAL SECURITY INFRASTRUCTURE

This section shall describe the infrastructure components (external/internal firewall, proxy, router, IDS/IPS, etc.) ensuring the peripherical security between the Contractor's network used for the data transmission network to the Commission and any other network (Internet, Partner, other office…).

2.1. Hardware components

<Description of the hardware platform for the above mentioned infrastructure components (external/internal firewall, proxy, router, IDS/IPS, etc.)>

2.2. Software components

<To be completed according to the §2.1: Filtering software type/product name/version or Operating System Name & version for running the filtering software, …>

2.3. Filtering Rules

<List of the rules in place on the filtering equipment>

SECURITY CONVENTION FOR REMOTE ACCESS.Part2

N°: <dg acronym>.<serial number>.T1[2]

Security Directorate reserved area, do not fill

Convention Version N°	
Date of Approval	
Approved by	
Signature	

[2] DG only fills DG acronym, serial number is assigned by HR.DS

Between

the European Commission,

represented for the purposes of the agreement by

- Mr. Guido VERVAET for the Security Directorate
- Mr. Marc FEIDT for the Directorate-General for Informatics
- ***<Authorised Person to sign>*** for ***<DG or Service>***

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 4

2. OBJECT 4

3. RULES 4

3.1. Authorised Staff 4

3.2. Authentication / Identification of the Authorised Staff 5

3.3. The Contractor environment 5

3.4. Contractor specific duties 5

3.5. Mutual undertaking 6

4. COMMISSION ENVIRONMENT 6

5. ANNEXES 6

ANNEX I RULES APPLICABLE TO THE MEMBERS OF THE AUTHORISED STAFF 9

ANNEX II AUTHENTICATION / IDENTIFICATION MECHANISM TO ACCESS THE RESOURCES DESCRIBED IN ANNEX V 10

1. ACCESS TO THE EC NETWORK 10

2. RESOURCES AUTHENTICATION / IDENTIFICATION MECHANISM 10

ANNEXE III DESCRIPTION OF THE INCIDENT HANDLING PROCEDURE 11

ANNEXE IV DESCRIPTION OF THE PROCEDURE USED TO SET-UP AND MAINTAIN THE CONNECTION 14

ANNEX V DESCRIPTION OF THE AUTHORISED REMOTE ACCESS 18

3. 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. This information in that document could not be added to this present document because of confidentiality of this kind of 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.

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

4. OBJECT

The present document set 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.

5. 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.

5.1. Authorised Staff

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

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

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

5.2. Authentication / Identification of the Authorised Staff

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

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

(8) 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.

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

(10) 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.

5.3. The Contractor environment

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

5.4. Contractor specific duties

The contractor undertakes:

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

(12) 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;

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

(14) 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;

(15) 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.

5.5. Mutual undertaking

Both parties to the agreement undertake:

(16) To inform each other[3] of any attack on the security mechanisms of their systems that could affect the security of the other;

(17) 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;

(18) 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.

6. COMMISSION ENVIRONMENT

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

(19) 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.

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

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

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

7. 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

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

Done at <location> at <date>
Each party acknowledging receipt of its copy

For the Contractor

Name:

Title:

For the Commission

Security Directorate	Directorate General
Name: Guido VERVAET	Name: <Authorised person>
Title: Head of Unit HR.DS.5	Title: <IRM or higher>
Name: Kaili KATMANN	Name: < Authorised person >
Title: ICT Security Analyst	Title: LISO of DG

Directorate-General for Informatics

Name: Marc FEIDT

Title: Head of Unit DIGIT.C.2

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)

Office JMO B2/074

Rue Alcide de Gasperi, L-2920 Luxembourg

Name: K KATMANN

Function: ICT Security Analyst

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

Telephone: +352 4301 37 410

Fax: +352 4301 34799

ANNEX I
RULES APPLICABLE TO THE MEMBERS OF THE AUTHORISED STAFF

Members of the authorised staff shall:

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

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

(25) 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;

(26) 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;

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

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

(29) 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;

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

(31) 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;

(32) 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;

(33) 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;

(34) 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

8. 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 Annexe II, 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.

9. 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 & authentication can be in place, usually a UserID/Password pair is used but others method as strong passwords can be necessary.

ANNEXE 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 local IRM team of the DG (in general from 9h00 to 17h30) for all kind of incidents. The contractor can only obtain aid by calling the local helpdesk of the DG.

Local Help Desk[4]:

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

Name of contact person: <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 central-helpdesk@ec.europa.eu or a Fax to +32 2 2963027
(2) Second, Call +32 2 2958181 (24h/24h 7d/7d)
- Press 1 to reach operator outside working hours [(20h -> 8h]
- Back-up number (+32) 0498/50.60.11

Important! E-mail and fax are 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 or fax
- each e-mail or fax must be clarified by a phone call

[4] Filled out by the Directorate General

Support set-up of the contractor[5]:

<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: …

FAX 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: …

[5] Filled out by the Contractor

ANNEXE 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[6]

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»

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

Administrative information used by the Contractor[7]

Commission: Corporate Infrastructure Services

Contact to return:

- The «receipt acknowledge» message when receiving a VPN hardware client[8]

- A VPN hardware client

Postal address:

European Commission

Directorate-General for Informatics

Corporate Infrastructure Services/Network Services

Office B-28 2/21

Rue Belliard 28, 1040 Brussels

Belgium

Name: DI SANTE MAROLLI

Function: Administrative Agent - Gestionnaire à finalité administrative

Telephone: +32 2 29 56271

Email: DI-SANTE-MAROLLI@ec.europa.eu

Fax: +32.22 99 05 80

[7] Filled out by the Commission

[8] 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[9]

Contractor: representative of the company

<Company name>

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

Name of the representative of the company: …

Function: …

Telephone: …

Email: …

[9] 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

Corporate Support and Training Services/User Access Administration

Office JMO B2/069

Rue Alcide de Gasperi, L-2920 Luxembourg

Name: F DEVILLET

Function: Head of Section

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

Fax: (+352) 4301 35559

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 Contract or specific contract : < Contract N° >		**<End Date>**
Specific agreement N°	**Task description[10]**	**<End Date>**
….	**….**	**….**

[10] Give a brief description of the tasks achieved

INBOUND NETWORK ACCESS TO THE COMMISSION'S IT RESOURCES

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.

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

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

12 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).

13 Access to the specific resource will be **blocked** as from this day on

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			

RESOURCES AUTHENTICATION / IDENTIFICATION MECHANISM [14]

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.

Table 3: Resources Authentication/Identification Mechanism on resource level (application/service/etc)			
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. A separate actions must be taken by the DG project manager for the creation of login on those servers.

OUTBOUND NETWORK ACCESS TO THE CONTRACTOR'S IT RESOURCES

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

15 Outbound connections may be authorised when the Data Transmission Network is ISDN, PSTN or leased line after consultation of the Security Directorate.

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

17 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).

CONTRACTOR'S ACCESS NETWORK AND IT RESOURCES USED FOR THE ACCESS TO THE COMMISSION'S IT RESOURCES

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

Table 6: Platform used by the Authorised Staff to initiate the connections to the Commission's IT resources[18]			
Type			**Indicate the choices** (Put an X, multiple choice is permitted)
Software Client	**Operating platform[19]**		
		Windows XP (32-bit)	
		Windows 7 (32-bit only)	
		Windows Vista (all released 32-bit versions)	
		MAC OS X 10.4 and higher (both Intel & PPC)	
		Linux (GLIBC_2.2 and libstdc++.so/ beta for 64 bit)	
Hardware Client			

[18] Simultaneous access to contractor IT resources and Commission IT resources (mentioned in the table below) is not permitted

[19] **Full support is given ONLY for one operating platform (i.e. Windows XP (32-bit), Q1-2010). Minimal support is given for the other OS platforms/versions.**