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]

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

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 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, logical and organisational protection measures and the contractor's network. The contractor's security posture must provide reasonable assurance that the associated risks are mitigated to an acceptable level.

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-II, the physical, logical and organisational measures put in place.

(2) The Contractor's network must be adequately protected against assessed risks. The Contractor must describe, in Annex III, his network architecture as well as the means that are put in place in order to mitigate the risks to the network.

In case of multiple locations, Annex I-III shall be completed for each location.

4. CONTRACTOR SPECIFIC DUTIES

The contractor undertakes to inform the Security Directorate of the Commission when there are relevant changes to the described security posture.

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 securely.

6. ANNEXES

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

Annex I	Physical and organisational security measures
Annex I	Logical and organisational security measures
Annex III	Network security measures

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

(e-Signatory in ARES)

Name: Kaili KATMANN

Function: ICT Security Analyst

(e-Signatory in ARES)

ANNEX I

PHYSICAL AND ORGANISATIONAL SECURITY 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.

I-1	The address(es) of the location from which the remote access to the Commission´s resource is possible. In case of multiple locations, Annex I-III shall be completed for each location.
I-2	Size of the company (i.e. number of employees).
I-3	General description of the location, e.g. location of the office(s) in the building, access/entry points (e.g. doors, windows).
I-4	Access control measures at access/entry points of the building inside and outside working hours, like keys, access cards, "pin-code", etc.
I-5	Access control measures for common areas and for special areas (e.g. office with the remote access workstation(s), server room, etc.) like keys, access cards, "pin-code", etc.
I-6	Authorization matrix with physical access rights (i.e. inventory of the users and their rights) is reviewed on a regular basis and updated when there is a change (e.g. updated job description, arrival or departure of an employee, etc.).
I-7	Monitoring activity with logging and reporting on physical access activity for special areas (e.g. office with the workstation(s), server room, etc.).
I-8	Video surveillance for common areas and for special areas (e.g. office with the workstation(s), server room, etc.).
I-9	Physical security measures for outside working hours when the areas are left unattended like intrusion detection system alarm or guards.

I-10	Specific organisational measures regarding physical protection (e.g. visitor policy or procedure when accessing office premises outside working hours).
I-11	Physical security measures for back-up storage.
I-12	Any other relevant physical or organisational security measure which aims to protect the premises.

ANNEX II

LOGICAL AND ORGANISATIONAL SECURITY 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.

II-1	Information security policy formally defined and adopted in the organisation, including risk management and the associated roles and responsibilities.
II-2	Information security management (either in general or for specific aspects) in the organisation certified for compliance with internationally recognised information security standards.
II-3	Information security audit/assessments or penetration tests performed (either by an internal service or a recognised external entity) on a regular or occasional basis.
II-4	General security principles applied in the organisation, e.g. "need to know", "least privilege", "segregation of duties", etc.
II-5	Authorization matrix with the user´s logical access rights (e.g. standard, privileged, administrator rights) is reviewed on a regular basis and updated when there is a change (e.g. updated job description, arrival or departure of an employee etc.).
II-6	Identification/authentication policies and access control infrastructure/mechanisms enforced on the devices (e.g. workstations, servers) through the organisation (including the devices which are giving access to Commission's resources).
II-7	Policy/security operating procedures defined and technical measures enforced for Wi-Fi access.
II-8	Policy/security operating procedures defined and technical measures enforced for removable media (e.g. usage of USB).

II-9	Alerts and/or regular reports with special events applied at any level (e.g. operating systems, applications, data bases & network equipments), like (but not only) access out of business hours, repeated failed login attempts, system settings changes, special privileges/actions, attacks and frauds. The usage of specific tools for the purpose of monitoring.
II-10	The hardening is applied on the devices (e.g. workstations, servers) like (but not only) HDD encryption, remove or stop unwanted components and all unnecessary applications, services and communication protocols, modify the registry and application settings known to be insecure, turn on auditing for all critical events, boot password.
II-11	The concept of reference/baseline configuration for devices is deployed in the organisation.
II-12	Password policy is defined and its compliance enforced by technical means, e.g. in respect of: ✓ requirements for pssword complexity ✓ password length ✓ password expiration period ✓ password history period ✓ number of failed login attempts that cause locked account ✓ successful/failed logging attempt events logged ✓ inactivity period of time that locks the computer
II-13	Measures against malicious code, i.e. the anti-virus/-spyware policy is enforced on all devices (e.g. workstations, laptops, servers, etc.) and updated on regular basis.
II-14	The patch management for operating systems and all the software is applied regularly and enforced with technical measures.
II-15	Policy/security operating procedures defined and technical measues enforced for the usage of private equipment for business reasons. Is BYOD allowed, what are the technical measures enforced and what resources can be accessed with private equipment?

II-16	Policy/security operating procedures defined and technical measues enforced for the mobile users / teleworkers. Is it allowed, what are the technical measures enforced and what resources can be accessed remotely? What are the security operating procedures in case of stolen/lost remote worker device?
II-17	Policy/security operating procedures defined and technical compliance check/health check (e.g. operating system patches installed, malicious code protection software state, firewall enabled, etc.) enforced on the devices which are connecting to corporate network (locally and/or remotely).
II-18	Company information security policy defines strategy in respect of awareness training for differnet target groups (e.g. system owners, end users, etc).
II-19	Any other relevant logical or organisational security measure which aims to protect the IT environment and the data processed therein.

ANNEX III
NETWORK SECURITY MEASURES

Describe the necessary security measures in place assuring the network protection of the resources from which the remote access to the Commission's resources is possible.

III-1	Architecture/topology - this section shall describe the topology of the network (up to its logical boundaries) to which the devices giving access to Commission's resources are connected. A network schema has to be provided below. The different networks with inbound or outbound connections to this network have to be represented such as the internet, interconnections wiht partners and/or service providers. Security mechanisms in place to protect the contractor's network boundaries have to be described.

<Network schema>

<table>
<tr><td rowspan="2">III-2</td><td colspan="4">Policy/security operating procedures defined and network access control infrastructure and mechanisms (e.g. external/internal firewall, gateway, router, IDS/IPS, etc.) implemented on the perimeter of the corporate network. The policy and its implementation is reviewed and verified on a regular basis and updated when there is a change.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="6">III-3</td><td colspan="4">The infrastructure components (e.g. external/internal firewall, gateway, router, IDS/IPS, etc.) ensuring the peripheral security between the company’s network used for the remote access to the Commission and any other network (e.g. internet, partner, other office).</td></tr>
<tr><td>Component</td><td>Brand</td><td>Model</td><td>Version</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">III-4</td><td colspan="4">Policy/security operating procedures defined and network segregation infrastructure implemented on the corporate network in order to satisfy business needs with different security requirements and avoid unauthorised access to information.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="2">III-5</td><td colspan="4">Policy/security operating procedures defined and network access control infrastructure and mechanisms implemented within the corporate network (for company and/or private devices).</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="2">III-6</td><td colspan="4">Policy/security operating procedures defined and contractual framework (including the relevant security requirements) established for usage of cloud based services.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="2">III-7</td><td colspan="4">Policy/security operating procedures defined and logging and monitoring implemented on the corporate network.</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td rowspan="2">III-8</td><td colspan="4">Any other relevant security measure which aims to protect the network.</td></tr>
<tr><td colspan="4"></td></tr>
</table>