EUROPEAN COMMISSION

DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY

Remote Service Delivery
Security baseline for external connections

Service providers with EC equipment (PXE)
Rules for contractors and service providers

Date:	22 April 2021
Version:	1.01
Authors:	
Revised by:	
Approved by:	

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: BERL 03/249 - Tel. direct line +32 229-57339

Commission européenne, 2920 Luxembourg, LUXEMBOURG - Tel. +352 43011

Table of Contents

1. Background 4

2. Scope 4

3. Approach 5

4. Commission responsibilities 5
4.1. Contract preparation 5
4.2. Commencement of services 6
4.3. Termination 6

5. References 7

6. Appendix 1 - Rules for Contractors 7
6.1. General rules 8
6.2. Access Control 9
6.3. Awareness and Training 10
6.4. Audit and Accountability 11
6.5. Security Assessment and Authorisation 12
6.6. Configuration Management 12
6.7. Identification and Authentication 12
6.8. Incident Response 13
6.9. Maintenance 13
6.10. Media Protection 13
6.11. Physical and Environmental Protection 14
6.12. Planning 15
6.13. Program Management 15
6.14. Personnel Security 16
6.15. Personally Identifiable Information Processing and Transparency 17
6.16. Risk Assessment 17
6.17. System and Services Acquisition 17
6.18. System and Communications Protection 17
6.19. System and Information Integrity 18

7. Appendix 2: Rules for Service Providers working from home 20
7.1. General rules 20
7.2. Access Control 20
7.3. Awareness and Training 21
7.4. Identification and Authentication 21
7.5. Incident Response 21
7.6. Media Protection 22
7.7. Physical and Environmental Protection 22
7.8. Personnel Security 23
7.9. System and Communications Protection 23

8. Appendix 3: Acceptable Use Policy 24

1. BACKGROUND

This document contains the baseline security measures for contractors[1] in the context of remote service delivery. It is one of a series of baselines that are published by the security directorate of DG HR (HR.DS) under Article 7 of Commission Decision C(2018)559[2].

The rules in this document specify the minimum security measures that contractors are required to put in place in order to mitigate risks to the security of Commission information during the fulfilment of the contracted services[3]. They focus mainly on the confidentiality and integrity of Commission equipment and information (measures to ensure high availability may also be relevant when required in the service level agreement but are out of scope of this document).

When the contractor undertakes to follow these controls in the contract, access is permitted without an additional Interconnection Security Agreement. **The Commission may verify the compliance with this baseline at any time**, either with its own staff or through the use of a third party (the cost is borne by the Commission unless stated otherwise in the contract).

2. SCOPE

The scenario covers the PXE scenario whereby service providers use Commission IT equipment (normally a laptop PC) and connect to the Commission's internal network via the remote access service for Commission staff. Service providers might be working on contractor premises (both near sites, in proximity to the relevant Commission office, or far sites, in any other EU location) or in home offices, where permitted by the contract. This baseline does not cover service providers accessing non-Commission systems, such as contractors' development environments.

The home office for a service provider must be located in an EU Member State and may be his/her own home or a similar location such as the residence of a relative or partner where the relevant security measures can be applied. Public spaces must not be used as home offices.

Where the controls refer to contractor or service provider equipment, this applies to the network equipment that is used for the connections to the EC Remote Access service (particularly the network switches, proxies, routers and boundary protection devices).

EU classified information (EUCI) is out of scope of this scenario. Any access to EUCI must follow the specific rules in place at the Commission.

---

1 In Commission terminology, the **contractor** is the company having a contract with the Commission, and a **service provider** is an individual consultant that works for the contractor.

2 Commission Decision (EU, Euratom) 2018/559 of 6 April 2018 laying down implementing rules for Article 6 of Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission (OJ L 93/4 of 11.4.2018

3 The relevant risks and high-level security requirements are laid out in the Standard on external network connections.

3. APPROACH

The general and specific rules in appendices 1 and 2 of this document must be followed by the contractor and its service providers respectively. The Commission will provide service descriptions and a set of facilities, as described in section 4 below, to enable the contractor to fulfil its security responsibilities.

The rules are partly based on the NIST Special Publication (SP) 800-53 (revision 5), Security and Privacy Controls for Information Systems and Organizations and the Commission's internal IT security standards, taking account of controls that are relevant for this scenario. The NIST publication was selected since it is publicly available, relatively detailed and considered as an industry standard. It is also used as a reference for security controls following a risk assessment using the Commission's ITSRM methodology.

Additional material has been included from version 7.1 of the "CIS Critical Security Controls", published by the Centre for Internet Security (cisecurity.org).

Contractors must implement the required controls and document their compliance or deviations, which may be requested or audited by the Commission at any time.

4. COMMISSION RESPONSIBILITIES

The Commission has a number of responsibilities to support contractors and service providers in the secure provision of external services. The key responsibilities relating to this document occur during contract preparation, at the start of a service provider's work (commencement of services) and at the end of a service provider's work (termination).

4.1. Contract preparation

During contract preparation:

- The contracting authority will describe the services to be provided by the contractor in the framework contract and/or in the service contract defining the scope of remote service delivery activities, personnel, hardware, software, sites and information to be exchanged, hosted and processed. The contract must include the obligations that the contractor has to impose on the service providers in the areas of information confidentiality.
- System owners must create service provider profiles (developer, tester, system administrator, project manager etc.) specifying the accesses required for the service providers to perform the remote service delivery, in line with the business requirements. The profiles include the basic network access and any addition access to Commission CISs that is needed.
- The requesting service in the Commission will inform the contractor which tasks are considered to be highly sensitive, and therefore what sort of screening is required (see controls PS-2 and PS-3 in appendix 1). The options are:
  i) Standard;
  ii) Highly sensitive (tasks requiring a security clearance).
- Commission system owners must ensure that all Commission CIS and services that are accessed by contractors under this scenario must take account of the risks and security

measures relating to their use by external personnel. This should be documented in the IT security plans of the systems accessed.

- Unless otherwise specified in the contract, the Commission IT equipment must only be delivered in person after the verification of the service provider's identity by the contracting authority. The standard IT delivery procedures apply.

4.2. Commencement of services

Before service providers start to work under the contract:

- the contracting authority will request the HR AMC to register the service provider in SYSPER under the code PXE, triggering the provision of the standard IT accesses including a unique network user ID, an email address on the @ext.ec.europa.eu domain and access to basic network services;
- the contracting authority will request the provision of the Commission IT equipment from DG DIGIT;
- HR.DS will ensure that the appropriate security screening is performed for the service provider as a part of the registration process.

On the first day of work under the contract (on Commission premises):

- A representative of the contracting authority will validate the service provider's identity and ensure that the service provider has signed the Acceptable Use Policy;
- the service provider, accompanied by a representative of the contracting authority, will collect the Commission IT equipment at the Commission's premises in Brussels or Luxembourg[4];
- HR.DS will provide a SECEM2 certificate; and
- at the request of the contracting authority, system owners will grant access to the Commission communication and information systems (CIS) as required for the contracted services with appropriate authorisations, in line with security principles (particularly least privilege).

During the first month of work under the contract:

- HR.DS &/or DIGIT will provide an introductory briefing on information security at the Commission.

4.3. Termination

Upon the termination of work of an individual service provider:

- all Commission IT equipment, access tokens/badges and any other Commission assets must be returned to the Commission's premises in Brussels or Luxembourg;
- system owners will immediately terminate all access granted to the service provider for the Commission's networks and CISs; and
- the contracting authority must check that these tasks have been performed correctly.

[4] Other Commission locations may be used to distribute the Commission IT equipment if a suitable agreement is in place between DIGIT, the contracting authority and the remote office to ensure that the proof of identity and the signature of the Acceptable Use Policy are verified.

5. REFERENCES

Description	Reference
The Commission's general security rules	https://myintracomm.ec.europa.eu/corp/security/EN/newDS3/PolicyLegislation/Pages/security-rules.aspx
The Commission's central IT security portal	https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Pages/default.aspx
The Commission's acceptable use rules for the use of IT resources	https://myintracomm.ec.europa.eu/infoadm/en/2016/Pages/ia16024.aspx
NIST SP 800-53 rev5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
NIST controls mapped to the EC's internal policies	http://www.cc.cec/wikis/pages/viewpage.action?pageId=398295430
CIS Critical Security Controls	https://www.cisecurity.org/controls/ [5]
CIS Initial Assessment Tool (v7.1c)	https://www.auditscripts.com/free-resources/critical-security-controls/

The Commission provides all relevant Commission documents to prospective tenderers during the procurement process.

6. APPENDIX 1 - RULES FOR CONTRACTORS

This section details all of the controls that are required for the security baseline. Each control includes its NIST ID and the title of the control area, and the specific security measures that are required by the Commission for this scenario. Contractors are advised to refer to the full NIST documentation for further information about the controls.

The technical controls in this appendix apply to the relevant network equipment owned by the contractor from where the connection to Commission systems is established, including any supporting systems, except where specified otherwise.

If the service providers do not work from contractor premises, the rules for working from a home office must be applied (see appendix 2).

The NIST Special Publication distinguishes the following security and privacy control families:

ID	Family
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability

[5] The CIS documents are licensed under a Creative Commons Attribution-ShareAlike 4.0 International License: http://creativecommons.org/licenses/by-sa/4.0/.

CA	Security Assessment and Authorisation
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PM	Program Management
PS	Personnel Security
PT	Personally Identifiable Information Processing and Transparency
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

6.1. General rules

(1) The contractor must cooperate with the Commission or any third party appointed by the Commission for the verification of compliance with these rules. The verification process may include on-site inspections in the contractor's premises.
(2) The contractor must have security policies covering all of the control families shown above.
(3) The contractor must nominate a single point of contact for security issues relating to the contract and to liaise with the Commission's security teams.
(4) The specific controls listed in this appendix must be implemented, and their implementation must be documented. Any exceptions must be documented and reported during any verification of compliance.
(5) Where a service delivery security plan is required in the contract, this baseline must be used as additional input for the security requirements.
(6) Contractors and their staff must be aware of the EC's security rules relating to their activities, the level of confidentiality of the information that they handle, and any relevant handling instructions (notably for sensitive non-classified information).
(7) Contractors must ensure that all service providers sign the applicable Acceptable Use Policy for the Commission IT equipment and follow any specific policies or rules for acceptable use relating to the CISs used.

(8) Commission information must not be stored or processed on any non-Commission devices or services without written authorisation from the Commission. Any such use is out of scope of this baseline and may be subject to different rules.
(9) The use of any online tools that are not authorised for use by the EC, such as instant messaging services or file storage/exchange platforms, is forbidden for handling, discussing or exchanging Commission information.
(10) Commission equipment and services must only be used for the fulfilment of services contracted for the Commission. All Commission equipment and information must be returned upon completion of the contracted services.
(11) In line with the standard contractual obligations, any non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.

6.2. Access Control

AC-2 Account Management

(1) All user accounts must be assigned to identified individuals. Shared accounts are not permitted.

For relevant network equipment owned by the contractor:

(2) Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.

(3) Configure access for all accounts through as few centralised points of authentication as possible, including network, security, and cloud systems.

(4) Encrypt or hash with a salt all authentication credentials when stored.

(5) Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

(6) Maintain an inventory of all accounts organized by the authentication system.

(7) Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.

(8) Disable any account that cannot be associated with a business process or business owner.

(9) Automatically disable dormant accounts after a set period of inactivity.

(10) Ensure that all accounts have an expiration date that is monitored and enforced.

(11) Monitor attempts to access deactivated accounts through audit logging.

For equipment/environment/CIS owned by the EC, the contractor must:

(12). Apply the Commission's procedures for requesting and reviewing access to Commission resources.

(13) Require approvals by EC account managers for requests to create accounts.

(14) Notify EC account managers when accounts are no longer required/users are terminated or transferred/system usage or need-to-know changes for an individual.

AC-5 Separation of Duties

Contractors must respect any segregation that is imposed by the CISs accessed.

AC-17 Remote Access

For remote access into the contractor's network environment (not using EC laptops):

(1) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed

(2) Authorise each type of remote access to the system prior to allowing such connections

(3) Route remote accesses through authorised and managed network access control points

(4) Require all remote login access to the organization's network to encrypt data in transit

(5) Use multi-factor authentication for remote access connections

(6) Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.

(7) Protect information about remote access mechanisms such as authentication methods from unauthorised use and disclosure.

AC-18 Wireless Access

For contractor sites:

(1) Maintain an inventory of authorised wireless access points connected to the wired network.

(2) Implement measures to detect and alert on unauthorised wireless access points.

(3) Disable wireless access on devices that do not have a business purpose for wireless access.

(4) Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.

(5) The Advanced Encryption Standard (AES) must be used to encrypt wireless data in transit.

(6) Ensure that wireless networks use secure authentication protocols based on the access scenario (i.e. which client is connecting and which network domains are accessed)

(7) Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.

(8) Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted, and filtered and audited accordingly.

6.3. Awareness and Training

AT-2 Literacy Training and Awareness

(1) The contractor must provide and keep records of security awareness training to its personnel, covering fundamental security issues.

(2) Service providers must also follow any security-related training required by the Commission, including initial briefings on information security and acceptable use of EC CIS and information.

6.4. Audit and Accountability

AU-2 Event Logging
(1) Ensure that local logging has been enabled on all systems and networking devices. (2) Log records must be made available to the Commission's security investigators in HR.DS in the event of a security incident.

AU-3 Content of Audit Records
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

AU-4 Audit Log Storage Capacity
Ensure that all systems that store logs have adequate storage space for the logs generated.

AU-6 Audit Record Review, Analysis, and Reporting
(1) Ensure that appropriate logs are being aggregated to a central log management system for analysis and review. (2) Deploy log analytic tools for log correlation and analysis (3) On a regular basis, review logs to identify anomalies or abnormal events.

AU-8 Time Stamps
Use at least two time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

AU-9 Protection of Audit Information
Protect audit information and audit logging tools from unauthorised access, modification, and deletion

AU-11 Audit Record Retention
Logs must be retained for at least six months.

6.5. Security Assessment and Authorisation

CA-2 Control Assessments
The security measures defined in this baseline must be assessed by the contractor or an independent assessor at least every three years. The results of this assessment must be made available to the contracting authority upon request.

6.6. Configuration Management

CM-2 Baseline Configuration
A secure configuration must be established for all relevant network devices.

CM-3 Configuration Change Control
A formal change control process must be in place for all relevant network devices.

CM-5 Access Restrictions for Change
Access to change configuration settings must be logged and restricted to qualified network administrators.

CM-8 System Component Inventory
All relevant network devices for the Commission access services must be identified.

6.7. Identification and Authentication

IA-1 Policy and Procedures
See rule (1) in section 6.1. Contractors must ensure the identity of their staff through suitable procedures.

IA-2 Identification and Authentication (organizational Users)
(1) Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorised individuals have elevated privileges. (2) Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. (3) Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account must only be used for administrative activities and not Internet browsing, email, or similar activities. (4) Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. (5) Use multi-factor authentication and encrypted channels for all administrative account access.

IA-5 Authenticator Management
(1) Credentials for access to the Commission must only be issued via a formal procedure including verification of the user's identity by the Commission (2) Credentials for access to contractor network devices must be issued via a formal procedure including verification of the user's identity

(3) Strong passwords (including requirements for minimum length and complexity) or multi-factor authentication must be enforced on the contractor's network

(4) Users must change passwords on first use (including default passwords for generic accounts, e.g. root, admin...)

(5) Passwords used to access the Commission's assets must be different from any other passwords of the user

(6) Users must protect all authenticators (passwords, laptops with digital certificate, tokens...) from unauthorised access, particularly when outside office premises (e.g. while working in home offices or travelling)

(7) Encrypt or hash with a salt all authentication credentials when stored.

(8) Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

6.8. Incident Response

IR-1 Policy and Procedures

(1) The contractor must have a documented incident response procedure.

(2) The contractor must appoint a single point of contact for communicating security incidents with the Commission.

(3) The contractor must report any relevant security incidents to the Commission's IT Helpdesk as soon as possible and cooperate with any security investigations.

(4) The contractor must ensure that any relevant evidence is preserved and made available to the Commission's security investigators in HR.DS.

6.9. Maintenance

MA-3 Maintenance Tools

Security updates must be applied in a timely manner to any relevant network equipment (OS and third party software)

6.10. Media Protection

MP-2 Media Access

The use of removable media for Commission information must be generally discouraged and restricted as much as possible. Where this is necessary, there must be specific rules over the handling and storage of the media, and the secure deletion of information when no longer needed.

At a minimum:

(1) Media must not be used for both Commission information and non-Commission information.

(2) Malware protection on Commission IT equipment must not be disabled or changed.

(3) Any Commission information at the level of Commission Use or above must be encrypted.

(4) Media must be physically protected when stored or transported.

(5) Any non-public Commission information must be securely deleted from removable media when no longer needed, or at latest at the termination of the contract.

(6) Users shall not connect media from unknown or suspicious sources to Commission IT equipment (e.g. media that are found unattended or received from unknown people)

MP-7 Media Use

Media that are not provided by the contractor or the EC must not be used for Commission information.

6.11. Physical and Environmental Protection

PE-1 Policy and Procedures

The physical security policy must cover (as relevant):

- Office spaces in contractor premises

- Home offices

- Data centres (for related network equipment)

Remote access to the EC environment is not permitted from any other locations.

PE-2 Physical Access Authorisations

Office spaces

(1) Office spaces must be designed to reduce physical risks such as eavesdropping, unauthorised observation of activities and loss or theft.

(2) Access must be restricted to authorised personnel (for visitor access see PE-7)

(3) There must be a formal process for granting access and revoking it when no longer justified

(4) Offices used for Commission work should be segregated from other offices, e.g. with access control or physical locks

Data centres

(5) As above, with access restricted only to relevant technical staff.

PE-3 Physical Access Control

Office spaces + Data centres

(1) All entrances and exits must be controlled (e.g. by access control systems or guards)

(2) Physical access control measures must be implemented as appropriate for both working and non-working hours

(3) Physical access logs must be retained for at least six months and made available to the Commission during security investigations.

PE-4 Access Control for Transmission
Physical network components including cables should be protected from unauthorised access.

PE-6 Monitoring Physical Access
(1) Office spaces and data centres on contractor sites must be monitored with intrusion alarms. (2) Entrances to data centres must be under video surveillance. (3) All alarms must be investigated as soon as possible.

PE-7 Visitor Control
Visitors to office spaces and data centres must be formally registered, with verification of their identity, and accompanied by an authorised user.

PE-8 Visitor Access Records
Records of visitor access must be maintained for at least six months and made available to the Commission during security investigations.

6.12. Planning

PL-2 System Security and Privacy Plans
The contractor must have up-to-date documentation covering: (1) the network architecture used for connecting to the EC's CISs (2) the provision of the contracted services.

6.13. Program Management

PM-1 Information Security Program Plan
See rule (1) in section 6. The contractor must have an information security management system in line with an appropriate security framework.

6.14. Personnel Security

PS-2 Position Risk Designation
The contracting authority in the Commission must inform the contractor which roles are considered to be sensitive, and therefore what sort of screening is required. The options are: i. Standard; ii. Highly sensitive (tasks requiring a security clearance).

PS-3 Personnel Screening
The contractor must provide the appropriate level of screening in line with the sensitivity of the tasks to be performed (see §4.1 above): The options are: i. Standard: contractor should have formal recruitment processes to verify the service provider's identity, education and work experience, including a criminal records check or equivalent (alternatively the EC can perform a background screening, where available - currently only in Belgium) ii. Highly sensitive: additionally, the contractor must apply for a national security clearance for the service provider as soon as possible. NB the Commission can only recognise security clearances for non-EU nationals of countries with which the EU has a Security of Information agreement or from a Member State that can clear non-EU nationals on their territory.

PS-4 Personnel Termination
(1) The EC must be informed of the termination of a service provider's contract to ensure that all user IDs are removed and any Commission assets are returned (laptop, hardware tokens, access badges etc.). (2) The service provider may be asked for a handover process &/or an exit interview and must be reminded of the continuing obligation to respect the confidentiality of Commission information.

PS-5 Personnel Transfer
When a service provider is transferred to a different role for the EC, the contractor must inform the EC to ensure that all access rights are modified accordingly. Transfer within the contractor to a non-EC role requires the same procedure as termination.

PS-7 External Personnel Security
Any relevant security requirements from the Commission must be included in the contract between the contractor and external personnel.

6.15. Personally Identifiable Information Processing and Transparency

PT-1 Policy and Procedures
If there are any GDPR-related requirements in the contract, these must be covered by the policy and any required security measures (e.g. if the contractor is acting as a data processor).

6.16. Risk Assessment

RA-1 Policy and Procedures
<u>For equipment/environment/CIS owned by the contractor:</u>

The contractor must have an ISMS in line with an appropriate security framework, including risk assessment in line with the requirements in the Call for Tender.

RA-5 Vulnerability Monitoring and Scanning
Vulnerability scanning must be performed regularly on the network equipment used for connecting to the Commission's infrastructure and a process must be in place to remediate any vulnerabilities identified.

6.17. System and Services Acquisition

SA-4 Acquisition Process
Relevant network devices must be procured through a formal process that includes security requirements

SA-5 System Documentation
Relevant network devices must be documented, including security requirements and configuration.

6.18. System and Communications Protection

SC-7 Boundary Protection
(1) Perform regular scans from outside each trusted network boundary to detect any unauthorised connections which are accessible across the boundary. (2) Deny communications by default, particularly incoming connections and known malicious or unused Internet IP addresses, and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries. (3) Deny communication over unauthorised TCP or UDP ports or application traffic to ensure that only authorised protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries. (4) Deny communications to/from unauthorised devices on the internal network. (5) Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries. (6) Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries. (7) Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. (8) Follow the control practices for external telecommunications services (see SC-7(4)). (9) Boundary protection devices must fail closed / secure. (10) Route traffic through authenticated proxy servers where possible.

(11) Secure network devices against unauthorised physical connections.

(12) Locate EC devices in a separate subnet / VLAN with restrictions on communications to/from the internal network.

SC-28 Protection of Information at Rest

EC information may only be handled on the provided EC equipment.

SC-35 External Malicious Code Identification

The contractor must have anti-malware protection at multiple levels (network, host…)

SC-43 Usage Restrictions

(1) Usage restrictions must be applied by the contractor in line with EC requirements. The contractor must ensure that all service providers sign and return the acceptable use policy provided by the Commission for the equipment provided.

(2) Only personnel employed on EC contracts may use EC equipment.

SC-45 System Time Synchronization

Contractor network equipment must be synchronised to a recognised external time source (and at least one other independent source for verification).

SC-46 Cross Domain Policy Enforcement

The VLAN in which the EC laptops reside must be restricted to communicating only with the EC, and protected from incoming communications from any other internal or external sources.

6.19. System and Information Integrity

SI-2 Flaw Remediation

A process must be in place for the timely identification and remediation of security vulnerabilities on relevant network devices.

SI-3 Malicious Code Protection

(1) The network environment must be protected from malware, including protection at the network perimeter.

(2) Anti-malware software must be centrally managed and regularly updated.

SI-4 System Monitoring

(1) The contractor must have intrusion detection and prevention on the network used for

connections to the Commission, with central management and alerting.

(2) The service must be regularly updated.

SI-5 Security Alerts, Advisories, and Directives

The contractor must monitor relevant security alerts for their environment.

7. APPENDIX 2: RULES FOR SERVICE PROVIDERS WORKING FROM HOME

This subset of the rules is applicable for service providers connecting from home offices. The home office for a service provider must be located in an EU Member State and may be his/her own home or a similar location such as the residence of a relative or partner where the relevant security measures can be applied.

7.1. General rules

(1) The specific controls listed in this appendix must be implemented. Any exceptions must be documented by the contractor and accepted by the EC as the contracting authority.

(2) Where a service delivery security plan is required in the contract, this baseline must be used as additional input for the security requirements.

(3) Service providers must be aware of the EC's security rules relating to their activities, the level of confidentiality of the information that they handle, and any relevant handling instructions (notably for sensitive non-classified information).

(4) Service providers must sign the applicable Acceptable Use Policy for the Commission IT equipment and follow any specific policies or rules for acceptable use relating to the CISs used.

(5) Commission information must not be stored or processed on any non-Commission devices or services without written authorisation from the Commission. Any such use is out of scope of this baseline and may be subject to different rules.

(6) The use of any online tools that are not authorised for use by the EC, such as instant messaging services or file storage/exchange platforms, is forbidden for handling, discussing or exchanging Commission information.

(7) Commission equipment and services must only be used for the fulfilment of services contracted for the Commission. All Commission equipment and information must be returned upon completion of the contracted services.

(8) In line with the standard contractual obligations, any non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.

7.2. Access Control

AC-2 Account Management
(1) All user accounts must be assigned to identified individuals. Shared accounts are not permitted. (2) Apply the Commission's procedures for requesting and reviewing access to Commission resources.

AC-5 Separation of Duties
Service providers must respect any segregation that is imposed by the CISs accessed.

AC-18 Wireless Access
(1) Users must be aware of the security of the digital environment used for remote access and take appropriate steps to reduce risks, including unauthorised access and malware infection. (2) Network devices that are used to access to Commission's resources must be protected by secure access control mechanisms. (3) Default passwords on network devices must be changed. (4) Users must not share the personal Wi-Fi Access Point with any unknown third parties.

7.3. Awareness and Training

AT-2 Literacy Training and Awareness
Service providers must follow any security-related training required by the Commission, including initial briefings on information security and acceptable use of EC CIS and information.

7.4. Identification and Authentication

IA-1 Policy and Procedures
Contractors must ensure the identity of their staff through suitable procedures.

IA-5 Authenticator Management
(1) Credentials for access to the Commission must only be issued via an agreed procedure including verification of the user's identity by the Commission (2) Users must change passwords on first use (including default passwords for generic accounts, e.g. root, admin...) (3) Passwords used to access the Commission's assets must be different from any other passwords of the user (4) Users must protect all authenticators (passwords, laptops with digital certificate, tokens...) from unauthorised access, particularly when outside office premises (e.g. while working in home offices or travelling)

7.5. Incident Response

IR-1 Policy and Procedures
(1) The service provider must report any relevant security incidents to the Commission's IT Helpdesk as soon as possible and cooperate with any security investigations. (2) The service provider must preserve any logs or other evidence of security incidents on Commission equipment.

7.6. Media Protection

MP-2 Media Access

The use of removable media for Commission information is generally discouraged and restricted as much as possible. Where this is necessary, there must be specific rules over the handling and storage of the media, and the secure deletion of information when no longer needed.

At a minimum:

(1) Media must not be used for both Commission information and non-Commission information.

(2) Malware protection on Commission IT equipment must not be disabled or changed.

(3) Any Commission information at the level of Commission Use or above must be encrypted.

(4) Media must be physically protected when stored or transported.

(5) Any non-public Commission information must be securely deleted from removable media when no longer needed, or at latest at the termination of the contract.

(6) Users shall not connect media from unknown or suspicious sources to Commission IT equipment (e.g. media that are found unattended or received from unknown people)

MP-7 Media Use

Media that are not provided by the contractor or the EC must not be used for Commission information.

7.7. Physical and Environmental Protection

PE-2 Physical Access Authorisations

(1) Users must be aware of the physical security of the environment where they are using remote access and take appropriate steps to reduce risks such as eavesdropping, unauthorised observation of their activities, and loss or theft of their equipment or credentials.

(2) Users must not store sensitive non-classified (SNC) information on non-Commission devices. Paperless working is recommended; printed documents containing SNC must be locked away when not in use.

(3) Users must not allow unauthorised people to use the device used for the Commission's remote access services, including friends and family members.

(4) Users must be attentive to signs of unauthorised use of endpoint devices. They must promptly report any suspected security breaches such as unrecognised access attempts via the appropriate channels.

PE-3 Physical Access Control

Home offices must be protected from intrusion, e.g. with locked doors on the premises. In shared homes, working in common areas is discouraged and Commission equipment must not be left unlocked or unattended.

7.8. Personnel Security

PS-3 Personnel Screening
The service provider must agree to the appropriate level of screening.

PS-4 Personnel Termination
(1) The EC must be informed of the termination of a service provider's contract to ensure that all user IDs are removed and any Commission assets are returned (laptop, hardware tokens, access badges etc.). (2) The service provider may be asked for a handover process &/or an exit interview and must be reminded of the continuing obligation to respect the confidentiality of Commission information.

PS-7 External Personnel Security
Any relevant security requirements from the Commission must be included in the contract between the contractor and external personnel.

7.9. System and Communications Protection

SC-28 Protection of Information at Rest
EC information may only be handled on the provided EC equipment.

SC-43 Usage Restrictions
(1) Usage restrictions must be followed by the service provider in line with EC requirements. The service provider must sign the acceptable use policy provided by the Commission for the equipment provided and return it via the contractor. (2) Only personnel employed on EC contracts may use EC equipment.

8. APPENDIX 3: ACCEPTABLE USE POLICY

All service providers must sign and return the acceptable use policy (AUP) shown below. The signed AUPs must be collected by the contractor and submitted to the contracting authority at the start of the contract.

The document is available in PDF format at [LINK TO BE CREATED].

Acceptable Use of European Commission Information and IT Resources

All service providers in the PXE (Provider-eXternal-IT Equipment) category must sign this document to indicate their agreement and return it to the relevant contracting authority in the Commission.

General Principles

1. The Commission provides information communication and technology (ICT) services for Commission business. The use of Commission IT resources for personal use or other business purposes is forbidden.
2. Service providers must be aware of the level of confidentiality of the information that they handle. Non-public Commission information must not be stored or processed on any non-Commission devices or services without written authorisation from the Commission.
3. Commission information that is not publicly available may not be shared with any personnel without a need-to-know to fulfil their contracted tasks for the Commission.
4. Paperless working is recommended where possible and particularly while teleworking from home. Printed documents containing sensitive information must be locked away when not in use.
5. Authentication mechanisms must be protected from use by unauthorised persons at all times. User IDs and authentication credentials are individual and must not be shared.
6. Service providers must use different passwords for accessing Commission CISs from any other passwords.
7. Service providers remain fully responsible for the supplied equipment and for the actions taken in their name. Service providers must inform the Commission immediately via the IT Helpdesk of any suspected or confirmed security incident or weakness. They must not test or exploit any security weaknesses, or seek to circumvent the security measures put in place by the Commission.

End user devices (workstations, laptops or other personal computing devices)

8. All Commission devices must be protected from access or theft by unauthorised persons at all times including during transport. In shared offices or homes, working in common areas is discouraged and Commission equipment must not be left unlocked or unattended.
9. Software from non-Commission sources must not be installed or used on Commission IT equipment. Service providers must not change the security configuration of the operating system and any other installed software.
10. Commission devices may only connect to authorised networks for the purpose of connecting to the Commission's remote access services. Authorised networks include:
    - the Commission's internal network or guest wi-fi when on Commission premises;
    - the contractor's internal network;
    - the service provider's home network while teleworking;
    - any authorised network service contracted by the Commission.

11. Service providers must not use any unauthorised online services for Commission purposes in the event that the Commission's teleworking solutions are unavailable.
12. Security measures installed on end user devices, including anti-malware software and firewalls, must not be disabled or their configuration changed.
13. Service providers must not allow unauthorised people to use the Commission's equipment or services, including friends and family members.

Commission communication and information systems (CISs)

14. The Commission's CISs must only be used for the provision of the services described in the contract and in line with the Commission's IT security policy and any rules or guidelines on acceptable use issued by the system owner.
15. Service providers must not access CISs for which they have not been explicitly granted authorisation.
16. Privileged access rights such as system administration must be used with extreme care. Service providers with administrative privileges must use a dedicated account for administrative tasks, and administrative accounts must not be used for any other activities.
17. Service provider must be vigilant of attacks such as phishing or scams.
18. Service providers must always encrypt sensitive non-classified emails with SECEM2.

Use of removable media and online services

19. The use of removable media for Commission information is strongly discouraged. All files must be securely deleted as soon as they are no longer needed.
20. Users shall not connect media from unknown or suspicious sources to Commission IT equipment.
21. Removable media containing Commission information must be protected against unauthorised disclosure, loss and theft. Security incidents involving removable media containing Commission information must be reported to the Commission via the IT Helpdesk.
22. Separate removable media must be used for Commission information and for other purposes.
23. Sensitive non-classified information must be encrypted on removable media.
24. Online services that are not provided or authorised by the Commission must not be used for communicating (videoconferencing / teleconferencing), storing or transferring Commission information.

Teleworking

25. Teleworking must only be performed from the service provider's home office which must be located in an EU Member State and may be his/her own home or a similar location such as the residence of a relative or partner where the relevant security measures can be applied. Teleworking is not permitted from public spaces such as hotels, restaurants, airports, train stations or social clubs.
26. When using home networks for teleworking, the following measures must be in place:
    - Home networks must not be shared with unknown persons;
    - Wireless networks must be encrypted and protected with a strong password;
    - Passwords used to access home networks, such as for wireless networks, must be changed from the default passwords;
    - Commission devices must not be connected to other home computing devices;
    - Commission devices must not be used to connect to the Internet except through the Commission's authorised networks.

Logging and monitoring

27. The service provider must accept that the supplied equipment will be subject to regular checks by the Commission; these may take the form of physical verification, user surveys and log consultation.
28. The service provider consents to the Commission logging and monitoring activities on its end user devices and CISs for security purposes. All such logs will be handled in accordance with the relevant privacy statements.

Termination

29. At the end of the contracted services, all Commission IT resources including end user devices, physical authentication mechanisms and information must be returned to the Commission.
30. All non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.

Confirmation

I hereby confirm that I have read, understood and will abide by the rules in this acceptable use policy.

Contractor company:	
Service provider (last name, first name):	
Signature:	
Date:	