Ref. Ares(2023)8815949 - 21/12/2023

EUROPEAN COMMISSION

DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY

Remote Service Delivery
Security baseline for external connections

Rules for contractors and service providers

Date:	17 August 2023
Version:	1.11
Authors:	K. Katmann, J. Oakey, A. Martins De Oliveira
Revised by:	G. Amato, N. Dubois, M. Meissl
Approved by:	B. Adolph

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

This document contains the baseline security measures for contractors ([1]) and service providers in the categories PPI, PPW, PXE and PXI when performing remote service delivery. This baseline is issued by the Security Directorate of DG HR (HR.DS) under Article 7 of Commission Decision (EU, Euratom) 2018/559 ([2]).

The categories are defined as follows:

- **P**rovider **P**remises **W**orkstation (**PPW**): Service provider with access to premises and a workstation (Commission office space and individual Commission IT equipment).
- **P**rovider **P**remises **I**T access (**PPI**): Service provider with regular IT access rights and regular access to buildings but that do not occupy a workstation.
- **P**rovider e**X**ternal IT **E**quipment (**PXE**): Service Provider hosted outside Commission premises with a "replicated" environment, Commission IT equipment and security measures.
- **P**rovider e**X**ternal **I**T access (**PXI**): Service provider with access to certain individually defined IT tools and systems to work remotely that do not need regular access to Commission premises, they do not have Commission IT equipment.

Additionally, there are two categories (PP – Provider Premises – and Not encoded) which do not have access to Commission information systems and are not covered by this baseline.

The rules in this document specify the minimal security measures that contractors are required to put in place 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). It should be noted that any security obligations on the contractors and service providers must be included in the relevant contracts, including in particular the compliance and verification requirements, in line with this security baseline.

The permitted modes for service delivery should be stipulated in the service contract, in particular whether remote service delivery is permitted (or even required), and under which conditions. Depending on the category (PPI, PPW, PXE, or PXI), the service provider may or may not be assigned Commission IT equipment. When the contractor undertakes to follow these security rules in the contract, access for PPI, PPW and PXE service providers is permitted without an additional Interconnection Security Agreement (ISA) ([4]). An ISA is still required for services provided with PXI service providers using custom interconnections, although this

([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 Standard C(2021) 8428 on External network connections (see https://ec.europa.eu/info/files/security-standards-information-systems_en)..

([4]) ISAs are defined in the Standard on External network connections.

baseline will simplify the ISA by replacing the previous part 1 of the ISA describing the contractor's security posture with the rules in section 6 below.

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

2.1. Provision of services

This security baseline covers all scenarios whereby service providers may perform remote service delivery, accessing Commission information in communication and information systems (CISs) on the Commission's internal network or in outsourced environments. Some of these categories of service providers use Commission IT equipment (normally a laptop) and connect to the Commission's internal network via the remote access service for Commission staff (PPW and PXE); the other categories (PPI and PXI) are not assigned a dedicated Commission end device but have IT access and may use non-Commission equipment to access Commission IT services remotely.

When performing remote service delivery, service providers may work in contractor premises or in home offices, where permitted by the contract.

Any remote service delivery site for a service provider must be located in an EU Member State (service providers may also exceptionally participate in missions outside the EU with authorisation from the Commission). A home office 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. Remote service delivery is not permitted from public spaces (e.g. hotel lobbies, restaurants, airports, train stations, social clubs…).

Where the controls refer to contractor or service provider equipment, this applies to the network equipment (particularly the network switches, proxies, (wi-fi) routers and boundary protection devices) that is used for the connections to the Commission's remote access services or Commission CISs.

2.2. Information handling

This baseline covers the handling of Commission information in transit and at rest on IT equipment or infrastructure used by service providers (including Commission or contractor laptops ([5]), the Commission networks and CISs to which they connect, and any removable media supplied by the Commission).

([5]) NB in this context, contractor laptops may only be used to access Commission CISs and may not be used to store Commission information.

The handling of Commission information in Commission CISs that are outsourced is out of scope. This is covered by the *Principles for outsourcing of communication and information systems* (C(2020) 4190 final).

This baseline does not cover the handling of information in other repositories or systems (including non-Commission removable media, contractors' file stores or cloud systems that are not Commission owned).

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

3. APPROACH

The general and specific rules in section 6 of this document must be followed by the contractor and its service providers as appropriate. Section 6 is split into two parts: the first part contains rules that are mandatory in all situations, and the second part contains additional scenario-specific rules for custom interconnections.

In addition, the contractor must ensure that all service providers sign the acceptable use policy in section 7 below, indicating the specific responsibilities of the individual service providers.

The Commission will provide service descriptions and a set of facilities (e.g. IT equipment, access passes and IT access) 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 remote service provision. 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 the "CIS Critical Security Controls", published by the Centre for Internet Security (cisecurity.org), and from the Commission's internal security policies.

Contractors must implement the required controls and document their implementation 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 and sites. The contract must include the obligations that the contractor has to impose on the service providers in the areas of information confidentiality and handling.
- The contracting authority will determine the appropriate category of service provider depending on factors such as the nature of the tasks and any security considerations.
- System owners must create service provider profiles (developer, tester, system administrator, project manager etc.) specifying the accesses required for the service providers to deliver services in line with the business requirements and the available network service offerings. The profiles include the basic network access and any additional 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 security verification is required (see controls PS-2 and PS-3 in section 6). 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 service providers 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.
- Commission IT equipment must only be delivered (where applicable) to new service providers in person after the verification of the service provider's identity by the service cards office. 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 relevant HR function to register the service provider in SYSPER under the relevant code (PPI, PPW, PXE or PXI), which will be the basis for the provision of building access rights, the relevant standard IT accesses in line with the service provider's category and the service requirements, such as a unique network user ID, an email address on the @ext.ec.europa.eu domain and access to basic network services;
- the service provider must sign the Acceptable Use Policy and send it to the contracting authority;
- where relevant, the contracting authority will make the necessary updates in PAX to enable the issuing of the pass granting access to Commission premises (the type of pass issued may depend on the category of the service provider);
- where relevant, the contracting authority will request the provision of the Commission IT equipment from DG DIGIT ([6]) (normally a laptop for PPW and PXE service providers);

([6]) DIGIT is the standard provider of Commission IT equipment but this task is delegated to local IT teams in some decentralised departments, such as the JRC.

- the contracting authority will enter the signed consent form in PAX to ensure that the appropriate security screening is performed for the service provider as a part of the registration process; and
- for third country service providers proposed by the contractor, the contracting authority will contact HR.DS to request a Third Country National Security Screening.

At the start of the contract:

- PPI, PPW and PXE service providers must make an appointment at the Service Cards Office for validation of their identity and issuance of an access badge;
- after this validation and where relevant, the service provider will collect the Commission IT equipment at the Commission's premises in Brussels or Luxembourg ([7]); and
- HR.DS will provide a SECEM certificate ([8]) when required (e.g. for email services or remote access authentication).

During the first three months of work for each service provider ([9]):

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

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).

The contracting authority must ensure that service providers are aware of the level of sensitivity of any information handled, and the corresponding handling instructions.

If service providers need to use removable media to store or handle Commission information, these must be supplied by the contracting authority.

If PXI service providers who do not possess an access badge need to come to the Commission's premises during the provision of services, they may obtain an access pass from the guards at building access points upon presentation of a valid national identity card or passport.

4.3. Termination

Upon the termination of work of an individual service provider:

- The contracting authority must ensure that all Commission assets (Commission information, laptop, hardware tokens, IT equipment, access badges etc.) are returned to the Commission;

([7]) Other Commission locations may be used to distribute the Commission IT equipment if a suitable agreement is in place between DIGIT (or the relevant delegated service), the contracting authority and the remote office to ensure that the proof of identity is verified.

([8]) SECEM is the Commission's S/MIME implementation.

([9]) Each service provider must follow the briefing once when they start to work for the Commission, or for existing service providers upon the adoption of this document. Service providers are not required to follow the briefing again for subsequent contracts.

- DIGIT must update the relevant equipment inventory records;
- the contracting authority must notify the system owners of CISs to which the service provider has access; and
- system owners will immediately terminate all access granted to the service provider for the Commission's networks and CISs.

These points must also be addressed as relevant when a service provider finishes a contract and begins a new contract with different tasks or in a different part of the Commission.

5. REFERENCES

Description	Reference
The Commission's general security rules	https://ec.europa.eu/info/files/security-standards-information-systems_en
NIST SP 800-53 rev5	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
CIS Critical Security Controls	https://www.cisecurity.org/controls/ ([10])

6. RULES FOR CONTRACTORS

These rules are split into two parts:

- The first part (section 6.1) contains rules that are applicable for all categories of service providers (PPI, PPW, PXE, PXI) and in all scenarios.
- The second part (section 6.2) contains additional rules that apply when the target Commission CIS (system, service or infrastructure) is not accessible by default via external gateways and requires a custom interconnection (covered by an ISA). Furthermore, the rules in section 6.2 apply on remote service delivery locations (on contractor premises) when equipment and devices that are owned by the contractor are used to access Commission CISs for the provision of services to the Commission.

The baseline controls are organised within the framework laid out in NIST SP 800-53. These controls are designed to be consistent with the security stance of the Commission's general security rules, while using publicly available standards for ease of reference.

Each control includes its NIST ID and the title of the control area, and the specific security measures that are required by the Commission. The controls in the security baseline are based on the NIST controls that are relevant for the provision of services to the Commission, with input from the CIS Critical Security Controls where necessary. Contractors are advised to refer to the

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

full NIST and CIS documentation for further information about the controls, although this is purely for guidance – only the rules given in this document are mandatory.

The NIST Special Publication distinguishes the following security and privacy control families (this baseline only includes the relevant families):

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

In addition, the security baseline starts with a number of general rules that are based upon the Commission's internal security and HR policies and which are not covered by the NIST control framework.

6.1. Baseline rules for all scenarios

The rules in section 6.1 are applicable to the contractor and, where specified, to the individual service provider. Rules that must be followed by the service provider are also specified in the Acceptable Use Policy in section 7 below.

These rules are applicable for all of the categories of service providers that are in scope of this security baseline (PPI, PPW, PXE and PXI) and for all contractors that provide these service providers. They apply to all working scenarios (including all locations, all types of end devices and all Commission systems and information accessed).

6.1.1. General rules

Ref	General rules
1	Any remote service delivery site for a service provider (contractor premises or home office) must be located in an EU Member State.
2	Service providers may also participate in missions outside the EU upon request from the Commission. In this case, service providers in collaboration with the contracting authority must obtain mission security advice in advance from the Security Directorate of DG HR and apply the recommended measures ([11]).
3	The contractor must nominate a single point of contact (SPOC) for security issues relating to the contract and to ensure the communication between the Commission's security teams and the relevant parties within the contractor.
4	Contractors and their staff must be aware of and comply with the Commission'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 (SNC) information, see https://europa.eu/!db43PX).
5	Contractors and their staff must not take Commission equipment or non-public Commission information outside the EU unless this is explicitly authorised for a mission to a non-EU country (see rule 2 above).
6	Contractors must ensure that all service providers sign the applicable Acceptable Use Policy (see section 7) and follow any specific policies or rules for acceptable use relating to the CISs used.
7	Commission information that is not publicly available must not be shared with any personnel without a need-to-know to fulfil their contracted tasks for the Commission.
8	Commission information that is not publicly available must not be stored or processed on any non-Commission devices or services.
9	The use of any public online tools that are not authorised for use by the Commission, such as instant messaging services or file storage/exchange platforms, is forbidden for handling, discussing or exchanging Commission information.

([11]) The measures for missions outside the EU depend on the circumstances of the mission and are out of scope of this document. Typically, they may include recommendations on working practices while on mission or measures such as the use of clean, dedicated IT equipment that is returned at the end of the mission.

Ref	General rules
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	Contractors and service providers should not permit seizure of Commission information or equipment by any non-Commission authorities or personnel, and must inform the Security Directorate of any such attempt.
12	In line with the standard contractual obligations, any non-disclosure or secrecy obligations continue to be binding after the completion of the contracted services.
13	The rules in this security baseline must be applied to any subcontractors who are involved in the delivery of (supporting) services.
14	The specific controls listed in section 6 must be implemented as relevant, and their implementation must be documented. Any exceptions or compensating controls must be documented and reported during any verification of compliance.
15	The contractor must cooperate with the Commission or any third party appointed by the Commission for the verification of compliance with these rules.
16	The process for the verification of compliance with these rules may cover: I. the documentation of the contractor's implementation of the specific controls; II. relevant security certifications of the contractor; III. the results of external audits/assessments; and IV. on-site inspections by the Commission in the contractor's premises. The contractor must provide the relevant evidence and access for this process.

6.1.2. Access Control

Ref	AC-2 Account Management
1	All user accounts in Commission CISs must be assigned to identified individuals. Shared accounts are not permitted unless an exception is authorised by the Commission system owner and accountability for each account is assigned to a specified individual.
2	Apply the Commission's procedures for requesting and reviewing access to Commission resources. All access requests must be documented, including the justification for access.
3	Where the administration of access management procedures for a Commission CIS is outsourced to the contractor, the Commission's internal rules on access management must be followed under the authority of the Commission system owner.

Ref	AC-2 Account Management
4	Notify Commission system owners when accounts are no longer required/users are terminated or transferred/system usage or need-to-know changes for an individual.

Ref	AC-5 Separation of Duties
1	Contractors and service providers must respect any segregation that is imposed by the CISs accessed.

6.1.3. Awareness and Training

Ref	AT-2 Literacy Training and Awareness
1	The contractor must provide and keep records of security awareness training to its personnel, covering fundamental and role-based security issues.
2	Service providers must also follow any security-related training required by the Commission, in particular the initial briefing on information security and acceptable use of Commission CISs and information that must be followed within three months of starting to work for the Commission.

6.1.4. Security Assessment and Authorisation

Ref	CA-2 Control Assessments
1	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.

Ref	CA-5 Plan of Action and Milestones
1	Develop a plan of action and milestones to document the planned remediation actions of the organisation to correct weaknesses or deficiencies noted during the assessment of the security measures, to be provided to the Commission upon request.

6.1.5. Identification and Authentication

Ref	IA-1	Policy and Procedures
1	The contractor must have formal recruitment processes to verify the service provider's identity, education and work experience, including a criminal records check or equivalent.	

Ref	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 as required by the system owner (in collaboration with the contractor where relevant).	

6.1.6. Incident Response

Ref	IR-1	Policy and Procedures
1	The contractor must have a documented incident response procedure.	
2	The contractor's single point of contact for security (see section 6.1.1, rule 3) must ensure effective communication between the contractor and the Commission regarding any relevant security incidents.	
3	The contractor and service provider must report any relevant security incidents to the Commission's IT Helpdesk without undue delay (within 48 hours), provide all relevant information and cooperate fully with any security investigations.	
4	The contractor must ensure that any relevant evidence is preserved and made available to the Commission's security investigators, including the results of the root cause analysis and any subsequent forensic examination.	
5	The Commission may instigate the compliance verification process following a security incident.	

6.1.7. Media Protection

Ref	MP-2	Media Access
1	The use of removable media for Commission information must be generally discouraged and restricted as much as possible.	
2	Commission information must only be stored on removable media provided by the Commission. These media must not be used for non-Commission information.	

Ref	MP-2	Media Access
3	Any Commission information on removable media at the level of sensitive non-classified (SNC) or above must be encrypted.	
4	Removable media containing Commission information must be protected against unauthorised disclosure, loss and theft.	
5	Any non-public Commission information must be securely deleted from removable media when no longer needed (e.g. by performing a full format), or at latest at the termination of the contract.	
6	Users must not connect media from unknown or suspicious sources to the IT equipment of the Commission or of the contractor (e.g. media that are found unattended or received from unknown people).	

6.1.8. Personnel Security

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

Ref	PS-3	Personnel Screening
1	The contractor must provide the appropriate level of screening in line with the sensitivity of the tasks to be performed and inform the Commission of the results. The options are: i. Standard: the contractor must have formal recruitment processes to verify the service provider's identity, education and work experience, including a criminal record check or equivalent. The Commission performs a background screening where available. ii. Highly sensitive: additionally, the contractor must apply for a national security clearance from a Member State or a recognised third country for the service provider as soon as possible. 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. HR.DS will perform the Third Country National Security Screening process for all service providers from non-EU countries.	

Ref	PS-4	Personnel Termination
1	The Commission 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 (Commission information, laptop, hardware tokens, IT equipment, access badges etc.).	
2	The service provider must be reminded of the continuing obligation to respect the confidentiality of Commission information.	

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

6.2. Rules dependent on working environment

The rules in this section apply when the target Commission CIS (system, service or infrastructure) is not accessible by default via external gateways and requires a custom interconnection (covered by an ISA). Furthermore, these rules apply on remote service delivery locations (on contractor premises) when equipment and devices that are owned by the contractor are used to access Commission CISs for the provision of services to the Commission.

6.2.1. General rules

Ref	General rules
1	The contractor must have security policies covering the rules in section 6.2 that are relevant to the working environment, taking into account the scope of the services provided and the associated risks.

6.2.2. Access Control

Ref	AC-2 Account Management
1	Maintain an inventory of each of the organisation's authentication and authorisation systems.
2	Centralise account management through a directory or identity service.
3	Ensure that all account usernames and initial authentication credentials are transmitted to users in a secure manner.

Ref	AC-2 Account Management
4	Maintain an inventory of all accounts organised by the authentication system.
5	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
6	Delete or disable any dormant accounts after a set period of inactivity.
7	Monitor failed authentications and attempts to access deactivated accounts through audit logging.

Ref	AC-6 Least Privilege
1	Contractors must ensure that service providers use accounts on end devices that apply the least privilege principle while accessing Commission information and CISs. In particular, the accounts used for these purposes must not have local administrative privileges.

Ref	AC-7 Unsuccessful Logon Attempts
1	The contractor must enforce a limit of consecutive invalid logon attempts on end devices that are used to access Commission CISs.

Ref	AC-11 Device Lock
1	The contractor must prevent unauthorised access to end devices through a device lock after a specified period of inactivity.

Ref	AC-17 Remote Access
	For remote access into the contractor's network environment:
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 organisation's network to encrypt data in transit.
5	Require multi-factor authentication for remote network access.

Ref	AC-17 Remote Access
6	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on factor such as: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up to date.
7	Protect information about remote access mechanisms such as authentication methods from unauthorised use and disclosure.

Ref	AC-18 Wireless Access
1	Establish and document configuration requirements, connection requirements, and implementation guidance for each type of wireless access before authorising wireless connections.
2	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).
3	Encrypt wireless data in transit using an appropriate secure encryption protocol.
4	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

6.2.3. Audit and Accountability

Ref	AU-2 Event Logging
1	Collect audit logs. Ensure that logging, per the contractor's audit log management process, has been enabled across all end devices, systems and networking devices (including boundary protection devices).
2	Log records must be made available to the Commission's security investigators in the event of a security incident.

Ref	AU-3 Content of Audit Records
1	Configure detailed audit logging to include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Ref	AU-4	Audit Log Storage Capacity
1	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	

Ref	AU-6	Audit Record Review, Analysis, and Reporting
1	Centralise, to the extent possible, audit log collection and retention across enterprise assets.	
2	Centralise security event alerting across enterprise assets for log correlation and analysis.	
3	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	

Ref	AU-8	Time Stamps
1	Standardise time synchronisation. Configure at least two time sources across enterprise assets, synchronised with a recognised external time source.	

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

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

6.2.4. Configuration Management

Ref	CM-2	Baseline Configuration
1	A secure baseline configuration must be established for all relevant end devices and network devices.	

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

Ref	CM-5	Access Restrictions for Changes
1	Access to change configuration settings must be logged and restricted to qualified system and network administrators.	

Ref	CM-6	Configuration Settings
1	Establish, document, implement and monitor configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements.	

Ref	CM-7	Least Functionality
1	Configure the system to provide only the required business functionality.	

Ref	CM-8	System Component Inventory
1	Develop, document and maintain an inventory of system components including end devices and network devices.	
2	Detect and alert the presence of unauthorised system components, and take appropriate actions, e.g. to disable or isolate them.	
3	All relevant end devices and network devices for the Commission access services must be identified.	

6.2.5. Identification and Authentication

Ref	IA-2	Identification and Authentication (organisational users)
1	Uniquely identify and authenticate organisational users and associate that unique identification with processes acting on behalf of those users.	
2	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. Validate that all active accounts are authorised, on a recurring schedule at a minimum quarterly, or more frequently.	
3	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	
4	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	

Ref	IA-2	Identification and Authentication (organisational users)
5		Use unique passwords for all enterprise assets including, at a minimum, an 8-character password for accounts using MFA and a 10-character password for accounts not using MFA (14 characters for privileged accounts).
6		Require MFA for all administrative access accounts, where supported, on all enterprise assets.

Ref	IA-5	Authenticator Management
1		Credentials for access to contractor end devices and network devices must be issued via a formal procedure including verification of the user's identity.
2		Strong passwords (including requirements for minimum length and complexity, see IA-2(5)) or multi-factor authentication must be enforced on the contractor's end devices and network.
3		User accounts must require passwords to be changed on first use (including default passwords for generic accounts, e.g. root, admin...).
4		All authentication credentials must be hashed with a salt when stored.

6.2.6. Maintenance

Ref	MA-2	Controlled Maintenance
1		Perform maintenance on organisational systems.
2		Ensure that equipment removed for off-site maintenance is sanitised of any Commission information.

Ref	MA-3	Maintenance Tools
1		Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

6.2.7. Physical and Environmental Protection

Ref	PE-1	Policy and Procedures
1	The physical security policy must cover (as relevant): - Office spaces in contractor premises - Data centres (for related network equipment)	
2	Paperless working is recommended; printed documents containing sensitive non-classified (SNC) information must be locked away when not in use.	

Ref	PE-2	Physical Access Authorisations
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	Access to data centres must be restricted only to relevant technical staff.	

Ref	PE-3	Physical Access Controls
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.	

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

Ref	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.	

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

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

6.2.8. Planning

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

6.2.9. Risk Assessment

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

6.2.10. System and Services Acquisition

Ref	SA-4	Acquisition Process
1	Relevant end devices and network devices must be procured through a formal process that includes security requirements.	

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

6.2.11. System and Communications Protection

Ref	SC-2	Separation of System and User Functionality
1	Separate user functionality, including user interface services, from system management functionality.	

Ref	SC-7	Boundary Protection
1	Monitor, control, and protect communications at the external boundaries and key internal boundaries of organisational systems.	
2	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal organisational networks.	
3	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 organisation's network boundaries.	
4	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 organisation's network boundaries.	
5	Boundary protection devices must fail closed / secure.	
6	Route traffic through authenticated proxy servers where possible.	
7	Secure network devices against unauthorised physical connections.	
8	Locate end user devices used for Commission purposes in a separate subnet / VLAN with restrictions on communications to & from internal and external networks.	
9	Do not allow remote devices to simultaneously connect to other systems or networks while they are connected to Commission remote access services (i.e. disable split tunnelling).	

Ref	SC-8	Transmission Confidentiality and Integrity
1	Implement cryptographic mechanisms to prevent unauthorised disclosure of or changes to Commission information during transmission.	

Ref	SC-43	Usage Restrictions
1	Usage restrictions must be applied by the contractor and followed by the service provider in line with Commission requirements. The contractor must ensure that all service providers sign and return the acceptable use policy provided by the Commission (see section 7).	

Ref	SC-43	Usage Restrictions
2	Only personnel employed on Commission contracts may use Commission equipment or services.	

Ref	SC-45	System Time Synchronisation
1	Contractor end devices and network equipment must be synchronised to recognised time sources (see control AU-8 Time Stamps).	

6.2.12. System and Information Integrity

Ref	SI-2	Flaw Remediation
1	A process must be in place for the timely identification and remediation of security vulnerabilities on relevant end devices and network devices, including the application of security updates.	

Ref	SI-3	Malicious Code Protection
1	The end devices and network environment must be protected from malware, including protection at the network perimeter.	
2	Anti-malware software must be centrally managed and regularly updated.	
3	End users must not disable or change the malware protection on IT equipment other than personal devices.	

Ref	SI-4	System Monitoring
1	The contractor must have intrusion detection and prevention on the network and its end devices used for connections to the Commission, with central management and alerting.	
2	The service must be regularly updated.	

Ref	SI-5	Security Alerts, Advisories, and Directives
1	The contractor must monitor relevant security alerts for their environment.	

7. ACCEPTABLE USE POLICY

This acceptable use policy contains rules to be followed by all service providers having access to Commission information or IT resources. All PPI, PPW, PXE and PXI service providers must sign this AUP to indicate their agreement. The signed AUPs must be collected by the contractor and submitted to the contracting authority at the start of the contract.

General Principles

1. The Commission provides information communication and technology (ICT) services for Commission business and the related security rules and handling instructions. The use of Commission information or IT resources for personal use or other business purposes is forbidden.
2. Service providers must give their assent to the appropriate level of screening during the recruitment process.
3. Service providers must be aware of the level of confidentiality of the information that they handle.
4. Commission information that is not publicly available must not be stored or processed on any non-Commission devices or services except as specified in the service contract, and it must not be shared with any personnel without a need-to-know to fulfil their contracted tasks for the Commission.
5. Paperless working is recommended where possible and particularly while performing remote service delivery. Printed documents containing sensitive information must be locked away when not in use.
6. Service providers must not take Commission equipment or non-public Commission information outside the EU unless this is explicitly authorised for a mission to a non-EU country.
7. Service providers must only use accounts that have been assigned to them. They must not share their accounts with other individuals or use shared accounts unless an exception is authorised by the Commission system owner and accountability for each account is assigned to a specified individual.
8. Authentication mechanisms must be protected from use by unauthorised persons at all times.
9. Service providers must use different passwords for accessing Commission CISs from any other passwords.
10. Service providers remain fully responsible for all equipment supplied by the Commission and for the actions taken in their name while using Commission equipment or services. Service providers must inform the Commission without undue delay (within 48 hours) 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.
11. Service providers must follow any security-related training required by the Commission, in particular the initial briefing on information security and acceptable use of Commission CISs and information that must be followed within three months of starting to work for the Commission.

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

12. All Commission devices must be protected from access or theft by unauthorised persons at all times including during transport.
13. In shared offices or homes, working in common areas is discouraged and end user devices used for Commission business must not be left unlocked or unattended.

14. 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.
15. Commission devices and contractor 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 (for Commission devices) or guest wi-fi (for contractor devices) when on Commission premises;
    - the contractor's internal network;
    - the service provider's home network or their personal mobile telephone hotspot while performing remote service delivery;
    - any authorised network service contracted by the Commission.
16. Service providers must not use any unauthorised or public online services for Commission purposes (e.g. in the event that the Commission's remote access solutions are unavailable).
17. Security measures installed on end user devices provided by the Commission, including anti-malware software and firewalls, must not be disabled or their configuration changed.
18. Service providers must not allow unauthorised people to use the Commission's equipment, information or services, including friends and family members.
19. Service providers 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.
20. Service providers must preserve any logs or other evidence of security incidents on any relevant IT equipment.
21. Service providers should not permit seizure of Commission information or equipment by any non-Commission authorities or personnel, and must inform the Security Directorate of any such attempt.

Commission communication and information systems (CISs)

22. 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.
23. Service providers must not access CISs for which they have not been explicitly granted authorisation.
24. 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.
25. Service provider must be vigilant of attacks such as phishing or scams.
26. Service providers using Commission devices must always encrypt sensitive non-classified emails with SECEM (or an equivalent authorised encryption tool).

Use of removable media and online services

27. 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.
28. Commission information must only be stored on removable media provided by the Commission. These media must not be used for non-Commission information.
29. Users must not connect media from unknown or suspicious sources to equipment that is used to access Commission services.
30. 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.

31. Sensitive non-classified information must be encrypted when stored on removable media.
32. Online services that are not provided or authorised by the Commission must not be used for communicating (videoconferencing/teleconferencing), storing or transferring Commission information that is not publicly available.

Remote service delivery

33. Remote service delivery must only be performed from contractor premises or 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. Remote service delivery is not permitted from public spaces such as hotel lobbies, restaurants, airports, train stations or social clubs.
34. Service providers 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.
35. 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 equipment must not be left unlocked or unattended.
36. When using home networks for remote service delivery, the following measures must be in place:
    - Home networks must not be shared with unknown third parties;
    - 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

37. 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.
38. The service provider consents to the Commission logging and monitoring activities on the Commission's end user devices and CISs for security purposes. All such logs will be handled in accordance with the relevant privacy statements.

Termination

39. 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.
40. The service provider must cooperate with a request from the Commission for a handover process &/or exit interview.
41. 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:	