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:	