Air Navigation Services of the Czech Republic

Amendment 3 to the Service Contract

Concluded pursuant to Section 1746 paragraph 2 of the Act No. 89/2012 Sb., the Civil Code, as amended (hereinafter referred to as the "**Civil Code**")

(Hereinafter referred to as the „**Amendment**")

1. Contracting Parties

Air Navigation Services of the Czech Republic (ANS CR)
With is registered office at Navigační 787, 252 61 Jeneč, Czech Republic
Represented by: [redacted]
Company Identification Number (IČO): 497 10 371
Tax Identification Number: CZ699004742
[redacted]

(Hereinafter referred to as the **"Client"**)

and

ROHDE & SCHWARZ – Praha, s.r.o.
With its registered office at Evropská 2590/33c, 160 00 Praha 6, Czech Republic
Represented by: [redacted]
Company Identification Number (IČO): 629 06 127
Tax Identification Number: CZ62906127
[redacted]

(Hereinafter referred to as the "**Contractor**")

(The Client and the Contractor hereinafter jointly referred to as the **„Parties**" and each individually as a **„Party**").

[redacted]

2. Preamble

2.1 On 26. 08. 2014 the Parties signed the Service Contract (Contract No. ANS CR: 280/2013/PS/030), as amended by the Amendment 1 dated 04.08.2016 and by the Amendment 2 dated 02.08.2017 (hereinafter referred to as the „**Contract“).**

2.2 Based on the fact that the Contractor has been identified as a significant contractor according to Section 2 (n) of the Regulation No. 82/2018 Sb., on security measures, cybersecurity incidents, reactive measures, requirements for filing in the area of cybersecurity, and data removal (Cybersecurity Regulation), the Parties agree to sign this Amendment, by which requirements of the Cybersecurity Regulation shall be implemented to the Contract.

3. Subject of the Amendment

3.1 With regards to the circumstances mentioned in Article 2.2 of this Amendment, the Parties hereby agree that Annex 1 to this Amendment, containing requirements of the Cybersecurity Regulation (i.e. information about security measures for contractual relationships with significant contractors pursuant to Annex 7 to the Cybersecurity Regulation), shall become integral and inseparable part of the Contract as a new Annex 3 to the Contract.

3.2 In Article 1.2 of the Contract, reference to the contract no. 351/2018/IS/086 shall be added. Based on this fact the Article 1.2 of the Contract shall be modified and shall newly be read as follows:

“1.2 The Service support shall mean performing repairs and/or interventions in the RCOM and VoIP VCS technology and information on upgrades (as further described in Articles 1.4., 1.5. and 1.6. and annexes to the Service Contract) supplied under the Contract for Work No. 279/2013/IS/080) and under the Contract for Work No. 351/2018/IS/086. Both mentioned contracts for work are hereinafter referred to as the “Contract for Work” and are known to and available for both Parties.

3.3 The price mentioned in Article 2.7.1 of the Contract shall be changed from [redacted] Based on this fact the Article 2.7.1 of the Contract shall be modified and shall newly be read as follows:

“2.7.1 RCOM technology

- *The Single fixed price for each repair (hereinafter the “SFPR^{RCOM}”) shall be:*

[redacted]

- *The Guaranteed average annual number of repairs of defects not caused by the Client’s or a third party’s fault guaranteed by the Contractor (hereinafter the guaranteed average annual number of repairs – GAANR^{RCOM}) shall be:*

[redacted]

3.4 The Client ´s phone number stated in Article 3.2.3.2 of the Contract shall be changed and shall newly be read as follows:

“3.2.3.2 The Client

Via telephone to service number [redacted]

by email to service email to: [redacted]

3.5 Article 3.2.7.4.3 of the Contract shall be modified and shall newly be read as follows:

"3.2.7.4.3. The Client is obliged to provide to employees designated by the Contractor remote access and VPN connection to maintained system via Customer CADIN IP data network based on defined access privileges. RSA SecureID token will be issued to each of these employees. The procedure of how to update a list of authorized persons is described in Article 4.2 of the Annex 1 to the Amendment 3 of the Contract".

3.6 The Article 10.5 and 10.6 of the Contract shall be removed with no replacement. The current Article 10.7 of the Contract shall be newly renumbered as Article 10.5 of the Contract.

3.7 New Article 10.6 of the Contract shall be added. The new Article 10.6. of the Contract shall be read as follows:

"10.6 Contact persons for the purposes of this Contract are as follows:

For the Client: [redacted]

For the Contractor:

The contact persons as stated above may in written form via email with electronic signature, databox or a letter sent via the holder of postal licence notify the other Party of additional contact persons, nevertheless such notification or the change of contact details shall be announced to the other Party without any delay.

Contact details of Cybersecurity manager shall be notified to the other Party by the contact persons as stated in this Article 10.6 of the Contract. These contact details/persons may be changed by the Parties from time to time nevertheless each change shall be announced to the other Party without any delay, and such communication shall be made between the contact persons stated in this Article 10.6 of the Contract in the form of letter sent via the holder of postal licence, databox or email with electronic signature."

3.8 The content of the current Annex 2 to the Contract (Secure ID Token Protocol) shall be replaced by the procedure described in Article 4.2 of the Annex 1 to this Amendment.

4. ISO27001 certification of the Contractor

4.1 In order to fulfil the requirements in Articles 3.1 – 3.5 and 4.1 - 4.3 of the Annex 1 to this Amendment, the Contractor (being the Provider) will undergo the ISO27001 Information Security system implementation and will pass ISO27001 certification procedure.

4.2 The adopted measures and procedures will cover the requirement of the Annex 1 to this Amendment and requirements listed in the Annex 2 to this Amendment.

4.3 The time schedule to introduce ISO27001 information security system in the Contractor´s (Provider´s) organisation will be as follows:

Implementation- before 30.09.2020

Certification - before 31.12.2020

4.4 During the implementation and certification period, the requirements of this Annex 1 and Annex 2 to this Amendment will not be enforceable from the Contractor (Provider).

5. Cyber security risk analyses of the concerned systems and related system changes

5.1 In order to identify the security gaps (technical) of the systems listed in the Article 1.2 of the Annex 1, based on the reasons stated in the Articles 1.6 – 1.8 of the Annex 1 to this Contract, the Client is obliged to conduct regular security risk analyses. The Contractor is

obliged to provide the Client with all available information and cooperation needed for that.

5.2 Based on the results of the above mentioned risk analyses, Client will take appropriate actions to improve the Cybersecurity of the concerned systems. Those actions may be a delivery of a system update, upgrade, reconfiguration or extension provided by the Contractor.

5.3 The time schedule for the risk analyses and system changes is anticipated by the Client to be as follows:

Risk analyses - 31.12.2020

Related system changes – 31.12.2021

6. Final Provisions

6.1 All the other Articles of the Contract shall not be changed by this Amendment.

6.2 This Amendment has been signed electronically, only in one electronic copy.

6.3 This Amendment shall be valid upon signature by the Parties and shall enter into force on the day when it is registered in the Register of Contracts according to Act. No. 340/2015 Coll., on the Register of Contracts, as amended.

6.4 Publication. The Contractor acknowledges that the Client is obliged to publish the Contract, the Amendment 1, the Amendment 2 and this Amendment 3 pursuant to the Act. No. 340/2015 Coll., on the Register of Contracts, as amended, and Act No. 106/1999 Coll., When the said documents are published in the Register of Contracts, in particular the following information contained in them shall not be provided:

For the Contract: Contractor´s bank details on the first page of the Contract, contacts and emails in Article 3.1.13.1, 3.1.13.2, 3.2.3.1 and 3.2.3.2 of the Contract, names in Article 10.5 of the Contract, signatures on the Contract, Annex 1 to the Contract because calculation contained in Annex 1 to the Contract is a trade secret within the sense of § 504 of the Civil Code.

For the Amendment 1: Contractor´s bank details on the first page of the Amendment 1, email and phone number in Article 1 of the Amendment 1, signatures on the Amendment No.1.

For the Amendment 2: Contractor´s bank details on the first page of the Amendment 2, emails and phone numbers in Article 3 of the Amendment 2, signatures on the Amendment No.2.

For this Amendment 3: Contractor´s bank details in Article 1 of the Amendment 3, signatures on the Amendment No.3., name of contact persons in Article 3.7 of this Amendment, technical details in Annex 2 to this Amendment.

6.5 The following Annex forms an integral part of this Contract:

- Annex 1 to this Amendment, which forms a new Annex 3 to the Contract – „Measures in the Area of Information and Cybersecurity pursuant to Regulation No. 82/2018 Sb., on security measures, cybersecurity incidents, reactive measures, requirements for filing in the area of cybersecurity, and data removal (Cybersecurity Regulation)

- Annex 2 to this Amendment, which forms a new Annex 4 to the Contract – „Security Rules for Major Contractors“

[redacted]

Director General

Air Navigation Services of the Czech Republic (ANS CR)

[redacted]

ROHDE & SCHWARZ – Praha, s.r.o.

Annex 1 to the Amendment 3 to the Service Contract No. 280/2013/PS/030 for the provision of service support for performance or repairs and/or interventions in the RCOM and VoIP VCS technology and information on upgrades (hereinafter referred to as the "Contract" or "Service Contract") Ensuring Measures in the Area of Information and Cybersecurity

"Contractual ensuring of measures in the area of information and cybersecurity within the meaning of Section 8 (2) of the Regulation No. 82/2018 Coll. on security measures, cybersecurity incidents, reactive measures, requirements for filing in the area of cybersecurity, and data removal (the Cybersecurity Regulation), as amended"

1. **Preamble**

1.1 The Provider understands and acknowledges that it is a significant contractor according to Section 2 (n) of the Cybersecurity Regulation for the Customer, which is Air Navigation Services of the Czech Republic (ANS CR) (hereinafter also referred to as the "Client" or "Customer"), who is an administrator of information and communication systems of the critical information infrastructure.

1.2 The following are the information/communication systems the role of a significant contractor relates to: **VoIP VCS, RCOM**.

1.3 The Provider undertakes to comply with the requirements of the information security management system specified in this Annex and in the security rules distributed in compliance with Article 6 hereof. The Provider within sense of this Annex is ROHDE & SCHWARZ – Praha, s.r.o., which is referred to as the Contractor in the Contract and the Customer is Air Navigation Services of the Czech Republic (ANS CR), which is referred to as the Client in the Contract.

1.4 The Provider shall comply with the following security rules in relation to all information / communication systems specified in Article 1.2 of this Annex. For other supported systems, compliance with security rules is reasonably required in accordance with best information security practice.

1.5 If any of the provisions of the Contract and its Annexes conflict with the provisions of this Annex or the security rules distributed in accordance with Article 6 of this Annex, the Provider shall proceed in accordance with the later provision.

1.6 The Client is aware also of his part of responsibility to achieve higher Cybersecurity level in the systems under the Service Contract and understands that fulfilling of the security rules only by the Provider is not sufficient to increase the complex Cybersecurity level of the systems noted in the Article1.2.

1.7 The Client is aware that the VoIP VCS and RCOM system delivered according to the Contract for Work ANS CR:279/2013/IS/080 - and being under the Service Contract - are not up to the state-of-the art level resilient against all Cybersecurity threats as the delivered system specifications had been created before these Cybersecurity requirements were enacted and imposed by law.

1.8 The Client is fully aware of the situation as stated in Articles 1.6 and 1.7 and he is ready to upgrade and extend the systems under the Service Contract up to conclusions of regularly conducted risk analysis.

2. **Definitions of Terms**

2.1 "Asset" shall mean a summary of information and services that are necessary for the operation of the information/communication system referred to in Article 1.2 hereof.

2.2 “Security Incident” shall mean violation of the information security in the information/communication system referred to in Article 1.2 hereof.

2.3 “Security Measure” shall mean an act the aim of which is to ensure information security in the information/communication system referred to in Article 1.2 hereof, its availability and reliability in the cybernetic space.

2.4 “Security Policy” shall mean a set of rules and principles determining the manner of ensuring of the assets protection, in particular according to Security Rules for Major Contractors referred to in Article 3.4 hereof.

2.5 “Security Event” shall mean an event that may violate the information security in the information/communication system referred to in Article 1.2 hereof.

2.6 “Provider” shall mean a significant contractor under Section 2 (n) of the Cybernetic Security Regulation.

2.7 “Critical Information Infrastructure” shall mean an element or a system of elements that are necessary for the operation of the information/communication system referred to in Article 1.2 hereof.

3. Information Security

3.1 The Provider is obliged to implement and realize Security Measures as required for ensuring of security of the information/communication systems referred to in Article 1.2 hereof and maintain appropriate security documentation in line with CSN ISO/IEC 27001 standard.

3.2 The Security Measures shall be set in compliance with the requirements of the Act No. 181/2014 Coll., on cybernetic security and on amendments to related acts (the Cybersecurity Act), as amended, the requirements of the Cybersecurity Regulation and possibly also of the CSN ISO/IEC 27001 standard.

3.3 The Customer shall verify the implementation and realisation of the Security Measures in compliance with Article 15 hereof or through a valid certificate of ISO/IEC 27001, or through a different established, valid and internationally recognized information security management system at the Provider.

3.4 The Provider shall take measures ensuring the confidentiality of data related to the provision of service support to the information/communication systems referred to in Article 1.2 hereof in compliance with the requirements of the Security Rules for Major Contractors distributed according to Article 6 hereof.

3.5 The Provider shall take measures ensuring the integrity of data related to the provision of service support to the information/communication systems referred to in Article 1.2 hereof in compliance with the requirements of the security rules distributed according to Article 6 hereof.

3.6 The Provider shall take measures ensuring the availability of data related to the provision of service support to the information/communication systems referred to in Article 1.2 hereof in compliance with the requirements of Article 3 of the Contract.

4. Authorization to Use Data, Rules of Access

4.1 The Provider shall be held liable for adherence to the rules of access as defined in Article 3.2.7.4.2 of the Contract, in Articles 4.2 hereof and the requirements of the security rules distributed according to Article 6 hereof.

4.2 The Provider shall especially be held liable for the timeliness of the list of workers authorized to enter the buildings and premises and access the

information/communication systems of the Customer. If the labour relation of a worker, who has access authorization, is terminated or if he/she is transferred onto a different position, the Provider shall inform the Customer of that fact without undue delay via the contact person whose name shall be notified according to Article 10.6 of the Contract. The list of authorised workers is distributed by an electronically signed e-mail to Customer´s Contact Person whose name shall be notified according to Article 10.6 of the Contract.

4.3 Communication in line with Article 4.2 hereof is to be conducted by electronically signed e-mails.

5. Copyright and Licence Rights

5.1 The Provider's obligations are defined in Article 6.1 of the Contract.

6. Adherence to Customer's Security Policies

6.1 The Provider shall make sure that all its employees who participate in performance of the obligations as defined herein or in the Contract have been provably acquainted with the Customer's Security Rules for Major Contractors (hereinafter the "Security Rules"), which will be distributed by electronically signed e-mails by the Customer's Cybersecurity manager whose name shall be notified according Article 10.6 of the Contract.

7. Compliance with Generally Binding Legal Regulations

7.1 The Provider undertakes to provide service support according to the Contract, in a due manner and in compliance with applicable standards and generally binding legal regulations applying to that kind of activity. The Provider shall hold the Provider liable for all damage arising out of a breach of those standards and regulations

8. Change Management

8.1 The Provider is required to manage risk associated with the performance of the Contract including residual risk. If requested by the Customer's Cybersecurity manager or by persons conducting the control activity as defined in Article 15 hereof, the Provider is required to document the risk management method.

8.2 The Provider understands and acknowledges that the Customer implements changes in compliance with Section 11 of the Cybersecurity Regulation.

8.3 As regards major changes, the Customer carries out a risk analysis in compliance with the CRAMM methodology, applying the RAMSES tool.

8.4 The Provider and all Subcontractors shall provide the Customer with necessary cooperation and shall be helpful during change management, especially during regular risk assessment and every inspection of the Security Measures implemented and realized by persons appointed by the Customer.

8.5 The Provider and all Subcontractors shall not provide for provision of the services under the Contract technical or programme tools of Huawei Technologies Co., Ltd. or ZTE Corporation including their subsidiaries.

9. Notification Requirements

9.1 The Provider shall inform the Customer without undue delay via the contact persons whose names shall be notified according to Article 10.6 of the Contract, if it identifies any

breach of the information security caused by a cyber incident and shall provide the Customer with sufficient information allowing to meet all requirements, respond to the incident, investigate it and report it to the National Cyber and Information Security Agency in compliance with the requirements of the Cybersecurity Regulation. The Provider is obliged to participate in such an effort and take financially reasonable steps requested by the Customer.

9.2 The Provider shall use the contact of the Customer´s Cybersecurity Team whose names shall be notified according to Article 10.6 of the Contract and inform the Customer on a continuous basis and without undue delay of all the threats and weaknesses the Provider is aware of that might impact the risk assessment carried out by the Customer.

9.3 The Provider shall inform the Customer´s Cybersecurity manager without undue delay of a major change in the Provider's control structure pursuant to the Business Corporations Act or of a change in the ownership of principal assets or of a change in the authorization to handle those assets used by the Provider for the performance of the Contract.

9.4 More detailed conditions of reporting and classification of security incidents are specified in the Security Rules distributed according to Article 6 hereof.

10. Continuity Management

10.1 The Provider shall ensure continuity in compliance with the instructions given by the responsible persons specified in Articles 3.1.13.2 and 3.2.3.2 of the Contract.

11. Terms of Data Handover

11.1 All operating data, databases, files, log content, other data and information provided and processed in connection with the subject matter of the Contract are the sole property of the Customer.

11.2 Data shall be transmitted in such a way, that unauthorized persons cannot read, copy, change or delete the data.

12. Subcontractors

12.1 In accordance with Section 105 (4) in conjunction with Section 3 of Act No. 134/2016 Coll., On Public Procurement, as amended, the Provider shall inform in writing in advance of its intention to use a subcontractor that the Provider has not notified during the procurement procedure, including its identification and details of the activities to be carried out by the subcontractor and the data made available. Identification of the subcontractors who will be involved in the performance of the public contract after the conclusion of the contract, the subject of activities to be performed by the subcontractor and the data made available shall be communicated by the Provider to the Client prior to commencement of performance by the subcontractor concerned.

12.2 If the Provider negotiates with a subcontractor to carry out activities or disclose data within the meaning of this Annex to the Contract, the Provider shall enter into a contract or other legal act with the subcontractor giving rise to the same rights and obligations in relation to information and cyber security as set out in this Annex. In particular, it is necessary to provide sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of the Regulation on Cyber Security.

12.3 In relation to each Subcontractor, the Provider shall:

a) Make reasonable effort to check that the Subcontractor provides the level of protection in the area of the information and cybersecurity as required by the Contract;

b) Make sure that in case of a chain of Subcontractors their mutual rights and obligations as regards the information and cybernetic security are regulated through a written contract including terms and conditions offering at least the same level of protection as those that are defined herein or in the Contract and meeting the requirements of the Cybersecurity Regulation;

c) Provide the Customer at its request with selected parts of contracts (or similar documents) concluded with the Subcontractors;

d) Make sure that every Subcontractor meets the obligations arising out of this Annex that apply to protection in the area of the information and cybersecurity executed by the Subcontractor as if the Subcontractor were a party to this Contract instead of the Provider.

12.4 In case that the Security Rules form an integral part of an agreement with subcontractors or between subcontractors, the Provider shall inform the Client in advance. The Client is entitled to object within five working days of the notification of the need to provide Security Rules to subcontractors that the provision of Security Rules to subcontractors is not necessary or that the provision of Security Rules to a specific subcontractor entails a security risk. In this case, the Provider must prove the necessary need to provide these Security Rules to a particular subcontractor or propose the use of another subcontractor. If the Client finds this need justified or fails to assess the new subcontractor as a security risk, the Client will allow to provide this safety information to the specific subcontractor.

13. Security Conditions upon Contract Termination

13.1 Upon the Contract termination, the Provider shall make sure that the terms and conditions determined in the Security Rules distributed under Article 6 hereof are complied with.

14. Data Removal Rules

14.1 Upon the Contract termination, the Provider shall make sure that the terms and conditions determined in the Security Rules distributed under Article 6 hereof are complied with.

15. Inspection

15.1 If requested, the Provider and all subcontractors shall provide access to all pre-agreed information required for proving of compliance herewith and cooperate during audits and inspections conducted by any auditor authorized by the Customer. The scope and range of the information audit shall be agreed in advance in written form by the Customer and the Provider.

15.2 The Customer shall inform the Provider of such an inspection well ahead of time prior to the inspection. In addition, the Customer shall make reasonable effort to make sure that the inspection will not be repeated more than one time per calendar year, will not take longer time frame than two working days and will not cause damage or disturb the premises, equipment, staff and activities of the Provider in an excessive manner. The Provider is not required to provide access to its premises during an inspection in the following situations:

a) The person conducting the inspection fails to present an identity card and an authorization to conduct the inspection;

b) The inspection is not conducted in the common working hours unless the inspection needs to be conducted beyond the common working hours and the inspector informed the Provider of that fact in advance (during common working hours).

15.3 The Provider understands and acknowledges that the Customer performs regular contractor assessment in compliance with the requirements of CSN EN ISO 9001 standard.

16. Contractual Penalties and Compensation for Other Damage

16.1 Sanctions provisions related to the Cybersecurity are listed in Article 7 of the Contract. If the Provider violates the remedial measures related to inspections according to Article 15 herein and further specified in the security rules distributed according to Article 6 herein, the Provider shall be duty-bound to pay a penalty 1900 EUR.

16.2 Payment of the contractual penalty is without prejudice to the entitlement to full damages.

16.3 Breach of the obligations determined in this Annex or in the Security Rules distributed under Article 6 hereof by the Provider may constitute a reason for unilateral termination of the Contract by the Customer.

17. Contact Details of Persons Responsible for Information Security

17.1 Contact details of the persons responsible for information security shall be notified according to Article 10.6. of the Contract.

Annex 2 to the Amendment 3 to the Service Contract No. 280/2013/PS/030 for the provision of service support for performance or repairs and/or interventions in the RCOM and VoIP VCS technology and information on upgrades

SECURITY RULES FOR MAJOR CONTRACTORS V1.0 (13.11.2019)

ACCORDING TO CZECH CYBER SECURITY LAW (181/2014 COLL.)

1. PERSONAL SECURITY

1.1. The contractual partner and its potential subcontractors (hereinafter referred to as "Contractor")

a) Shall have a Security Awareness Development Plan in place, the aim of which is to ensure adequate training and security awareness development and which contains the form, content and scope of the following:

i. Instructions for users, administrators, persons performing security functions and contractors concerning their obligations and the security policy;

ii. Required theoretical and practical training of users, administrators and persons performing security functions;

b) Shall have appointed persons responsible for realization of the individual activities listed in the plan;

c) Shall instruct, in compliance with the Security Awareness Development Plan, users, administrators and persons holding security roles on their obligations and on the security policy by means of initial and recurrent training;

d) In compliance with the Security Awareness Development Plan, ensure for persons holding security roles regular professional training based on the current needs as regards cybersecurity;

e) Shall ensure, in compliance with the Security Awareness Development Plan, regular training and verification of the employees' security awareness according to their job responsibilities;

f) Shall ensure inspections of compliance with the security policy by users, administrators and persons holding security roles;

g) Shall ensure handover of responsibilities if the contractual relationship with the administrators and persons holding security roles is terminated;

h) Shall evaluate the efficacy of the Security Awareness Development Plan, of the training having been realized as well as of other activities related to development of the security awareness;

i) Shall determine rules and procedures to deal with cases of breaches of the established security rules by users, administrators and persons holding security roles;

j) Shall keep records of training containing the subject matter of the training and a list of persons who attended it.

1.2. Air Navigation Services of the Czech Republic (hereinafter referred as "ANS CR") reserves the right to keep records of and check the Contractor's activities, keep records of incidents and unusual activities of the employees and other persons operating in favour or on behalf of the Contractor (hereinafter referred to as "Contractor's Staff"). Based on those records, ANS CR shall be entitled to evaluate the trustworthiness and reliability of the Contractor's Staff. In the event of any identified risk, the ANS CR shall inform the Contractor of a non-conformity and both parties shall enter into dealings to solve the situation.

9.4. The Contractor continuously monitors (within its ICT infrastructure) published and known security vulnerabilities which can influence smooth and safe operation of the systems covered by the Contract. It means for example vulnerabilities in the operation systems, third party software, web components etc.

10. PROTECTION OF MEDIA

10.1. The storage of ANS CR protected data on portable media and transfer of thereof outside premises of ANS CR requires prior approval of ANS CR.

10.2. In case of ANS CR protected data storage on portable media the Contractor is required, if manageable, to store or require the storage of such data encrypted and to keep records of these media.

10.3. The Contractor is required to ensure erasure of ANS CR protected data immediately after the purpose for their processing and/or storage has expired by the means of NIST 800-88 standard. It shall not be possible to recover the information after the data has been erased. The Contractor must keep a record of data erasure.

11. SECURITY EVENTS/INCIDENTS

11.1. The Contractor is required to report any suspicion of cybernetic security incidents:

a) To the respective ANS CR Technical Hall Supervisor;

b) Immediately after identifying the cybernetic security event/incident;

c) By e-mail, phone or in person;

d) With description

i. of the date and time of event/incident

ii. event/incident nature;

iii. of the source of the event/incident;

iv. of the target / victim of the event/incident;

v. of the potential impact.

12. AUDIT OF THE CONTRACTOR (CUSTOMER AUDIT RULES)

12.1. AUTHORIZATION TO PERFORM AUDIT OF THE CONTRACTOR

a) ANS CR reserves the right to perform audits of the Contractor.

b) ANS CR shall inform the Contractor of its intention of performing the audit at least 5 working days beforehand. Both parties shall agree upon the audit content, necessary cooperation and schedule and ANS CR undertakes to act so as not to disturb the Contractor's operation.

c) In case of any serious circumstances (e.g. suspicion of risky behaviour of the Contractor) related to the performance of this contract, ANS CR reserves the right to perform an unannounced audit of the Contractor taking into consideration the Contractor's operating circumstances.

d) When critical information infrastructure elements related to respective implementing Regulation (EU) laying down common requirements for air traffic management / air navigation services providers and other functions of the air traffic management network are audited and supervised (by provision of ANS), the auditor / inspector

1.3. The qualification of the Contractor's Staff must correspond to the work position occupied (to the work performed and the level of security).

2. PHYSICAL SECURITY AND SAFETY

2.1. The Contractor as an employer in performance of the respective contract is responsible for complying with Safety and Health Protection and Fire Protection regulations by its employees or other individuals engaged in work in its favor (hereinafter together referred to as "the Contractor´s employees"). [redacted] Any damages resulting from violation of these regulations by the Contracting Partner´s employees shall be borne by the Contractor. If the Contractor generates dangerous places or situations on site as a result of its activity, the Contractor shall take his own measures to secure the impending damage and shall immediately inform ANS CR of this fact.

2.2. When executing the subject of performance, the Contractor shall be obliged to respect the terms and conditions of entry of persons and vehicles in the premises, buildings and lands of ANS CR and the security regime determined for them. Those terms and conditions are especially defined in ANS CR internal regulations called Regime of Entry of Persons and Vehicles in the Premises and Buildings of RLP CR, s.p. and in the Non-Public Area of Airports, Rules and Conditions for External Entities in the Premises and Buildings of RLP CR, s.p., and in the applicable operating rules. The Contractor's Staff are acquainted with those rules by the Ordering Party's staff. In association to the operating needs and the risk assessment, entry is realised in several security regimes:

a) Unaccompanied Entry. This kind of entry is designed for Contractor´s employees with operational need to access ANS CR facilities on a regular basis. Entry is granted after completing the Application for ANS CR permanent identification card and attendance of ANS CR security awareness training. During the security awareness training, the document Rules and conditions for Contractor´s employees is given to each participant. This document summarizes basic security rules for given type of access rights. Obligatory precondition for permanent identification card issuance is presentation of an extract from criminal record register not older than 3 months (alternatively valid civil aviation Background check or National security clearance certificate of CONFIDENTIAL or higher level may be presented). Issuance of the card is charged. After the termination of the respective contract or termination of employment relation or other relation to Contractor by the respective Contractor´s employee, the Contractor is obliged to return issued identification card to designated office of ANS CR. ANS CR reserves the right to terminate the validity or withdraw the permanent identification card for security reasons at any time.

b) Partial unaccompanied Entry. This kind of entry is designed for Contractor´s employees when operational circumstances do not allow permanent escort of the employee by permanent identification card holder. Entry is granted after visitor card issuance and after being demonstrably aware of the rules specified in the document Rules and conditions for Contracting Partner´s employees, which summarizes basic security rules for given type of access rights. The person, who has granted the access for the visitor by his/her permanent identification card, is responsible for observation of security conditions by the visitor. ANS CR reserves the right to terminate the right of partly unaccompanied entry of certain person or group of persons for security reasons at any time.

c) Accompanied entry to ATM related premises. This kind of entry is applicable at all other circumstances at the facilities or premises designed for the provision of ATM services. Entry is granted after visitor card issuance. The person, who has granted the access for the visitor by his/her permanent identification card, is

responsible for observation of security conditions by the visitor. ANS CR reserves the right to terminate the right of accompanied entry of certain person or group of persons for security reasons at any time.

d) Unacompanied entry to other ANS CR non ATM premises (Air Navigation Institute, recreational facilities, etc). This kind of entry is regulated by the code of entry issued by the building/premises administrator.

3. SECURITY AWARENESS

3.1. All Contractor's Staff must be provably trained and acquainted with the applicable internal documents of the Ordering Party relating to the subject of performance of this contract. The Contractor is responsible for training of the Contractor's Staff and for acquainting them with the requirements of this contract and the annexes thereof.

4. IDENTIFICATION

4.1. All Contractor's Staff who participate in the performance of the contract through the Contractor's ICT technology must have their own unique user account recorded and maintained within their ICT infrastructure, while every such user account shall be associated with specific roles in the individual systems, modules or applications. All Contractor's Staff must have valid identification and current contact details.

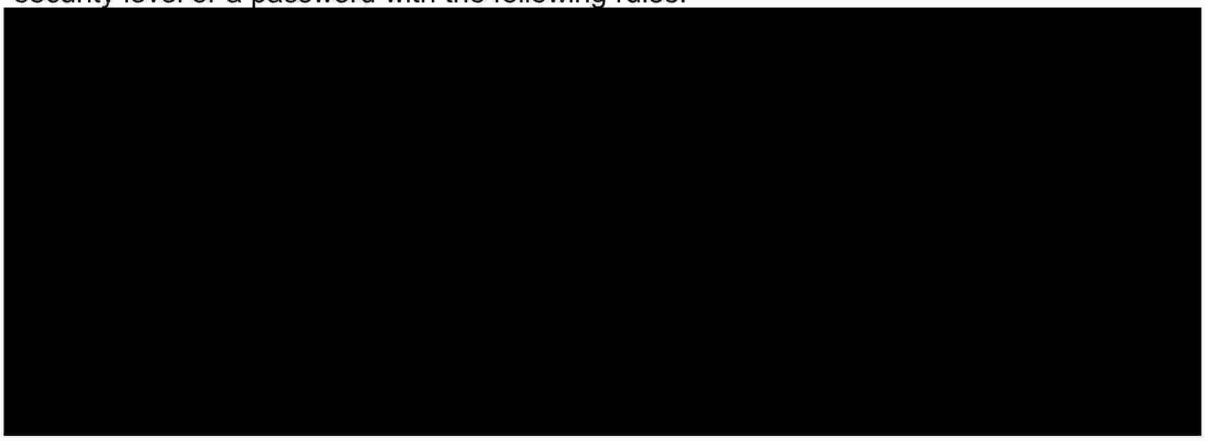
4.2. All Contractor's Staff who access the Ordering Party's internal ICT systems shall have their unique user account kept and maintained by the Ordering Party, and specific roles associated exclusively with the performance of the subject of this contract are to be assigned to every such account in the individual systems, modules or applications.

5. AUTHENTICATION

5.1. Terms for authentication within the ANS CR ICT infrastructure:

a) Multi-factor authentication is used for identification of system maintenance workers and administrators.

b) Password-based verification - where clear multi-factor identification cannot be used, it is necessary to use authentication through cryptographic keys guaranteeing a similar security level or a password with the following rules:



5.2. As regards remote access of the Contractor, the Contractor shall submit documents for completion of an application for remote access according to which the following security rules are set afterwards:

a) The technical administrator of the respective system of ANS CR shall complete the application on behalf of the Contractor (based on source documents provided by the Contractor's contact person);

b) The application content must be fully in line with the subject of performance of this contract;

[redacted]

5.3. [redacted] the Contractor guarantee that all his [redacted] which they have been acquainted with. Any damages resulting from violation of these rules by the Contractor´s employees [redacted] shall be borne by the Contractor.

6. AUTHORIZATION

6.1. The Contractor's staff using ANS CR ICT infrastructure are required to use the privileged authorization reasonably and only for a period of time that is necessary for performance of the activities in line with the subject of the contract. Users and administrators are not allowed to use privileged authorization accounts for common work that is not related to the information system administration.

6.2. ANS CR shall inform the Contractor's Staff of the ANS CR protected information they have access to and the manner they can handle it. The Contractor is not allowed to handle the Ordering Party's protected information in a manner or conduct that are not explicitly listed in the instructions.

7. WORKSTATION SECURITY

7.1. Access to ANS CR information systems is realized by means of the ANS CR equipment (HW, SW) by default.

7.2. The Contractor's HW (PC, laptops) can only access internal protected information and ICT systems if approved by the respective ANS CR workplace and responsible technical administrator.

7.3. The Contractor´s HW connected to ANS CZ via VPN must:

a) Have a functional anti-virus certified by AV-TEST (av-test.org) or VB100 (virusbulletin.com);

b) Have a functional personal firewall (FSCS);

c) Have functional and set automatic system updates (Windows Server Update Services);

d) Have an operation system that is covered by the producer's service support (if this is not explicitly excluded by contractual agreement);

e) Have conditions ensured in the Linux environment similar to those for Windows as defined above - AV, FSCS, UPDATE, OS.

8. USE OF CRYPTOGRAPHIC TOOLS

8.1. If the use of cryptographic tools is required within the subject of performance, the technical conditions are as follows:

a) Symmetric password encryption applying [redacted] The password must be submitted by a different communication channel;

b) Encryption by means of digital certificates issued by a generally recognized CA or by a CA that is explicitly trusted by both parties;

c) If the certificate validity towards CRL cannot be verified, the certificate shall be considered invalid and cannot be used for encryption or signing;

d) Encryption using PGP keys approved by both parties or verified by an independent trustworthy third party;

e) [redacted] or a stronger one shall be used for the VPN access to

f) A HTTPS protocol with a cypher of [redacted] shall be used for web servers presenting data from [redacted] beyond the system itself;

g) AN EV certificate of a generally recognized certification authority shall be used for web servers presenting data from [redacted] for users out of ANS CR.

9. MONITORING

9.1. Access of the Contractor's Staff to selected internal information and to the information and telecommunication systems is recorded, monitored and evaluated on a continuous basis.

9.2. The following system events are recorded in logs:

[redacted]

9.3. For every log entry following meta data are assigned by ANS CR:

[redacted]

establishes corrective measures to findings and date to be implemented. The Contractor is obliged to implement the corrective measures within the scope of the stipulated corrective measure and the required deadline.

e) Audit documents shall be maintained by ANS CR Internal Ivestigation and Audit Department. Records of a particular audit shall always be provided with the same identifier. The individual audit records consists of:

   i. Audit plan;

   ii. Audit notification;

   iii. Audit questionnaire (a list of auditor's questions if the auditor considers it appropriate);

   iv. Audit report;

   v. Written, picture or other records of the operation, procedures or equipment related to the audit (if necessary for documenting of the findings);

   vi. Record of findings (remedial measures and subsequent check).

f) The audited party (the Contractor) shall receive a final audit report including potential findings:

   i. Based on the findings listed in the final audit report, the Contractor shall propose remedial measures and deadlines and submit a list thereof to ANS CR for approval;

   ii. ANS CR shall confirm the measures proposed.

12.2. REMEDIAL MEASURES

a) The audited party (the Contractor) is required to ensure implementation of the arranged remedial measures by the deadline arranged.

b) The Contractor shall submit the report of the measures implemented to ANS CR.

13. TERMINATION OF THE CONTRACT ARRANGEMENTS

13.1. In case of termination of the Contract, all Contractor´s access to ANS CR assets (VPN, systems, applications, data) are terminated not later than at the last day of Contract validity.

13.2. If the assets of ANS CR have been provided to the Contractor (authentification token, workstation, laptop, etc.) all items must be returned not later than the last day of Contract validity.

13.3. If the ANS CR data assets (data) have been provided to the Contractor, all data has to be returned and erased from all Contractor´s information systems and media by the means of NIST 800-88 standard .

13.4. In case of a non-standard termination of the Contract, if necessary, Contractor´s access may be terminated before the contractual agreement expires.

END