Air Navigation Services
of the Czech Republic

Service support for Surface Movement Radar

concluded pursuant to Section 1746, paragraph 2 of the Act No 89/2012 Coll., Civil Code, as amended

(hereinafter referred to as the “**Civil Code**”)

(hereinafter referred to as the “**Contract**”)

1. Parties

Air Navigation Services of the Czech Republic (ANS CR)
a state enterprise existing and organized under the laws of the Czech Republic
having its registered office at: Navigační 787, 252 61 Jeneč, Czech Republic
Company Identification Number: 49710371
Tax Identification Number: CZ699004742
Bank Connection: Československá obchodní banka, a.s.
Account Number: 8815080/0300
IBAN: CZ04 0300 1760 3000 0008 8153 SWIFT code: CEKOCZPP
Registered in the Commercial Register of the Municipal Court in Prague, Section A, Insert 10771,
[redacted]

(hereinafter referred to as the “**Customer**”)

and

Saab., Inc.
Seated at 85 Collamer Crossings East Syracuse, NY 13057, USA
Represented by: Stephen Furcinito, Senior Contracts Manager
Company Identification Number: 2717452
Tax Identification Number: 58-2310523
[redacted]

(hereinafter referred to as the “**Provider**”)

(the Customer and the Provider hereinafter jointly referred to as the “**Parties**” and each individually as a “**Party**”)

2. Preamble

WHEREAS

2.1 the Customer has a need for correct functioning of Surface Movement Radar SR-03 that is necessary for proper provision of air navigation services, and for that purpose has an interest in service support for such Surface Movement Radar,

2.2 the Provider as the supplier of the Surface Movement Radar SR-03 is able to provide requested service support, has the knowledge and skills to provide it in the highest available quality, is able to and shall act with the knowledge and diligence usually associated with its profession or status, meets all conditions and requirements stipulated in this Contract and is entitled to enter into the present Contract and duly meet the obligations contained herein,

the Parties agree on entering into the present Contract.

3. Subject of the Contract

3.1 The Provider agrees to provide the Customer with the following service support for Surface Movement Radar SR-03 (hereinafter referred to as "**SMR**") owned by the Customer:

3.1.1. Customer Service and Project Management,

3.1.2. Technical support,

as further specified in this Contract (hereinafter referred to as "**service support**").

3.2 The Customer agrees to pay the Provider for the service support the price as stated in Article 6 of this Contract.

4. Service Support Description

4.1 Customer Service and Project Management

4.1.1. The Provider shall provide a single point of contact, by phone and email, to quickly log, track and route all issues and requests from assignment through closure.

4.1.2. The following contact information can be accessed on a 24x7 basis:

4.1.2.1. Email: customerservice@saabinc.com

4.1.2.2. Phone: +01 315-445-5000

NOTE: Critical situations, which require immediate response, should be reported through the phone system. Issues received via email will be responded to next business day.

4.1.3. The Customer Problem Report (CPR) shall be used as the primary mean to initiate all support actions for technical concerns/issues.

4.1.4. Upon receipt of a Customer call or email by Provider Customer Service, a Customer service representative shall log the request into the Product Support Database. The Customer Service representative then assigns the reported Technical issue to the appropriate representative to begin resolution. For each CPR form sent by the Customer, the Provider shall inform the Customer about the CPR number and confirm the critical or non-critical status of the CPR within 1 business day.

4.1.5. Customer Service shall be available 24 hours per day, 7 days per week, 365 days per year.

4.1.6. Some issues may be resolved directly with Customer Service, other issues may require help from Technical Support as further specified in Article 4.2 of this Contract.

4.2 Technical support

4.2.1. If an open CPR requires support from a Provider engineer or SMR expert, the Provider shall provide remote technical support to the Customer to assist in resolution of system issues that prevent the system from meeting specified performance requirements resulting from a system defect (i.e. hardware failure or software bug). Upon receipt of a technical issue, a Provider Technical Support Representative shall be assigned to respond to Customer's representative to review, investigate and resolve the reported issue.

4.2.2. Technical support shall be provided by a qualified Provider engineer via phone, email, or other electronic means. Each Technical support issue shall be classified by the Customer and upon receipt confirmed by Provider Technical Engineer as critical, serious or non-critical.

4.2.3. The Provider shall assign the CPR to Technical support person within 1 business day of notification. The issue shall be resolved as quickly as practical, depending on the level of severity of the issue.

4.2.4. Technical support in the scope of 40 man-hours a year is included in the fix price stated in Article 6.1.1 of this Contract. If more than 40 man-hours of Technical support is required in a given year, those man-hours shall be ordered by the Customer and paid in accordance with Article 6.4.2 of this Contract.

5. Place of performance

5.1 The SMR for which the service support is provided is located at following Customer`s premises:

5.1.1. IATCC Praha, Navigační 787, 252 61 Jeneč,

5.1.2. Technical building, Václav Havel Airport, Aviatická 1039, 160 08 Prague.

6. Prices and payment

6.1 The maximum price of the service support according to this Contract is

[redacted]

and is composed of following items:

6.1.1. price for Customer Service and Project Management and Technical support in the scope of 40 man-hours per year which amounts to [redacted] excluding VAT per one month, 6.1.2. price for Technical support above the treshold as stated in Article 6.1.1 of this Contract which amounts to:

[redacted]

6.2 The Prices stated in Article 6.1.2 of this Contract shall be escalated 3% per Contract year. The Provider shall notify the Customer in written form the escalation of the price according to this paragraph when sending the invoice, which reflects such price escalation at the latest, otherwise the price escalation shall not be applied. Such notification shall be sent by the Provider on the address for sending the invoices according to paragraph 6.5 of the Contract.

6.3 The prices mentioned in this Contract are expressed excluding VAT, including all other taxes, customs duties and fees.

6.4 The service support shall be invoiced to the Customer by the Provider as follows:

6.4.1. Payments for the service support according to Article 6.1.1 of this Contract shall be made in the form of semiannual payments in June and December for the service support provided in past half-year. The first payment shall be made in the aliquot part of the year. Payments shall be made on the basis of invoice – tax document. A statement of actually performed man-hours and Report on Technical support shall be attached to the invoice.

6.4.2. Payments for Technical support according to Article 6.1.2 of this Contract shall be paid on the basis of actually performed man-hours in relevant half a year. A statement of actually performed man-hours and Report on Technical support shall be attached to the invoice. This payment will be made on the basis of an invoice issued by the Contractor in June and December for the above threshold Technical support provided in past half-year

6.5 The invoice maturity shall be thirty (30) days from the date of its receipt by the Customer. Upon an authorized return of an invoice, the maturity period stops running on the day of sending the invoice and a new maturity period starts upon the delivery of a corrected or completed invoice. Each invoice, marked with the ANS CR contract number, which is located in the heading of this Contract, and attachments according to Article 6.4 of this Contract, must be sent in written form on the address of the Customer as stated in Article 1 of this Contract, or via email from Provider`s email address [redacted] to Customer`s email address [redacted] otherwise it shall be returned to the Provider.

7. Taxes

7.1 The Provider declares that its domicile is in United States of America.

7.2 The Customer declares that its domicile is in the Czech Republic.

7.3 The contractual total price has been calculated and is expressed excluding of VAT, which, if any, shall be borne by the Customer. VAT shall be applied in accordance with the Act. No. 235/2004 Coll., on Value Added Tax, as amended.

7.4 All terms of payment according to the Contract shall be subject to the tax laws of the Czech Republic and Double Taxation Agreement between the Czech Republic and United States of America.

7.5 The Customer is not responsible for any Provider obligations to tax offices of the Czech Republic.

8. Obligations and responsibilities

8.1 The Provider as an employer in performance of this 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. Any damages resulting from violation of these regulations by the Provider’s employees or other individuals engaged in work in its favor shall be borne by the Provider.

8.2 The Customer shall provide to the designated Provider’s employees or to other persons performing the work on behalf of the Provider (hereinafter together referred to as the “Provider 's employees”) remote access and VPN connection to the maintained system via Client’s IP data network (CADIN) based on defined access privileges. A RSA SecureID token will be issued to each of these Provider’s employees, a list of which shall be delivered in a written form to the Customer before the need of remote access to Customer's system, against the signature of each designated Provider’s employee. The list of the designated Provider’s employees may be changed by the Provider from time to time, nevertheless each change shall be announced to the Customer without any delay, and such communication shall be made between the contact persons stated in Article 15.1 of this Contract in the form of letter sent via electronic (digital) means, such are an e-mail message, where attachments shall be converted to pdf format and signed by a certified electronic signature (according to eIDAS), or the data box or by paper-based mail via a postal licence holder with confirmation of delivery.

8.3 The Provider as an employer is responsible for its employees to observe the Customer’s rules for VPN access when using RSA SecureID tokens (issued based on Article 8.2 of this Contract) and also for the loss of RSA SecureID token. The Customer is obliged to provide the Provider with VPN access rules. The Provider is obliged to compensate all damages caused by breaking these rules by its employees. The rules for VPN access are available at:

https://www.ans.cz/content/documents/Security_rules_for_major_contractors.pdf

8.4 Given that the Provider was evaluated as a major contractor within the meaning of Section 2 (n) Regulation No. 82/2018 Coll., on security measures, cybersecurity incidents, reactive measures, requirements for filing in the area of cybersecurity, and data removal, as amended (hereinafter referred to as the "Cyber Security Regulation"), the Parties agree that an integral part of this Contract is the Annex 1 of this Contract which contains the requirements of Annex 7 of the Cyber Security Regulation (i.e. information regarding security measures for contractual relations with major contractors). The Provider shall fulfil the obligations set out in the Annex 1 of this Contract. Contact details of cyber security manager shall be notified to the other Party by the contact persons as stated in Article 15.1 of this 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 Article 15.1 of this Contract in electronic (digital) form, meaning email with attachments converted in pdf format and signed with recognized electronic signature (in accordance with eIDAS), in the form of letter sent via the holder of postal licence with confirmation of delivery or databox.

8.5 The Provider shall ensure, through the responsible person, that obligation stated in Article 8.3 and 8.4 of this Contract are known to persons engaged in activities related to this Contract.

8.6 The Client shall provide the Provider with necessary assistance upon request.

8.7 The Parties are obliged to maintain confidentiality towards third parties about all confidential facts that they have learned about in connection with this Contract. The Customer considers all data stored in systems and programs of the Customer as confidential, for unlimited period of time. The Provider is not allowed to provide such information and/or data to third person.

9. Intellectual property

9.1 The Provider warrants that the service support provided according to this Contract does not infringe any third-party rights (patents and other industrial and intellectual property rights).

9.2 All intellectual and/or industrial property rights relating to the service support shall, subject to any rights of third parties, remain exclusively with the Provider.

9.3 The Provider hereby grants the Customer a right to use all the author crafts that originate in connection with the service support of the Provider in conformity and conditions of this Contract. The licence is granted as non-exclusive, unlimited and non-transferable licence to use SMR for its purpose.

9.4 For avoidance of any doubts, the Parties hereby declare, that all data, configurations, user settings or templates created by means of the software or contained therein, shall be subject to intellectual property rights of the Customer and the Provider shall be entitled to use them during performance of this Contract on the basis of explicit instruction given by the Customer.

10. Warranty

10.1 The Provider guarantees that it shall provide up to 180 days warranty from acceptance for any software adjustments and supplements.

10.2 These warranty will not apply:

10.2.1. if adjustment, repair, or parts replacement is required due to accident, unusual physical or electrical power, air conditioning, humidity control, or causes other than intended ordinary use, 10.2.2. if the equipment and/or the system into which it is installed has been modified by the Customer, or

10.2.3. if adjustment of the equipment and/or the system into which it is installed is required due to a change in the external environment that is not within the control of the Provider.

10.3 Should it be determined upon the completion of the reported warranty work that such work falls outside the scope of this warranty, the Provider shall be entitled to bill the Customer on a time basis at rates according to Article 6.1.2 of this Contract for all work accomplished.

10.4 Unless stated otherwise in this Contract the liability for defects follows the Section 2615 et seq. of the Civil Code.

11. Liability

11.1 Either Party shall defend, indemnify, and hold the other Party harmless from any and all claims, losses, expenses, costs or damages directly arising from the injury to or death of any person and the damage to or loss of any property, which it has caused in the framework of this Contract.

11.2 The Provider shall be liable to the Customer for damages which arise directly from the performance, incorrect performance or non-performance of the Provider duties and obligations under this Contract.

11.3 Limit of liability - In no event shall Provider be liable for incidental, indirect, special, punitive or consequential damages, including, without limitation, lost profits revenue, business opportunity or loss to other machinery or equipment of which a product of Provider is a part, regardless of the form of action, whether in contract, tort (including negligence), strict product liability or otherwise, even if Provider has reason to know or has been advised of the possibility of such damages.

12. Force MAJEURE

12.1 Each Party shall not have any legal liability to the other Party if it cannot perform its obligations under this Contract for a cause of force majeure i.e. any event that is beyond its reasonable control. In such a case, the Party, which is prevented from fulfilling its contractual obligations by the force majeure event, shall give notice of the event and the time set forth in this Contract will be extended by the number of days necessary to overcome the causes of the delay. Performance under and performance of this Contract shall be resumed as soon as practicable after such event has come to an end. If the performance of whole or part of this Contract is delayed by reason of force majeure for a period exceeding three (3) months, either Party may request termination of this Contract or the affected part thereof. Then the Parties will endeavour to establish by mutual agreement on the termination of the contractual relationship; failing such an agreement, provisions of Article 14 of this Contract hereafter shall apply.

13. Term

13.1 This Contract is concluded for a period of 5 years starting from its entry into effect.

14. Dispute settlement

14.1 The Parties agree that all and any disputes arising from this Contract shall be settled by an amicable agreement. If no such agreement can be reached, such dispute shall be referred to an independent court.

14.2 This Contract is governed by laws and legal procedures of the Czech Republic.

14.3 All and any disputes arising from or related to this Contract shall be referred to a competent court in the Czech Republic. The Parties hereby agree that a court of Customer´s registered office shall be considered appropriate.

15. Contacts

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

[redacted]

15.2 The contact persons as stated above may provide the other Party with the list of further contact persons or its amendment. A list of designated contacts shall be sent by electronic (digital) means, such are an e-mail message, where attachments shall be converted to pdf format and signed by a certified electronic signature (according to eIDAS), or the data box or by paper-based mail via a postal licence holder.

16. Assignment – subcontracting

16.1 Neither Party to this Contract shall be entitled to assign or transfer any of its contractual rights or obligations to any third party without prior written approval from the other Party; such approval shall not be denied unreasonably. The Provider shall be entitled to subcontract, under its responsibility, any part of this Contract.

17. Termination

17.1 Either Party is entitled to terminate the Contract if the other Party materially breaches its obligations under the Contract by notifying the other Party thereof in writing. The Party receiving the notification of termination shall have 60 days to remedy the failure described in the notification to the satisfaction of the issuing Party. The following actions, with the possibility of withdrawal from the Contract, are deemed to be a material breach of the Contract:

17.1.1. the Provider breaches the provision of Annex 1 of this Contract or Security Rules notified pursuant to Article 4 of Annex 1 to the Contract,

17.1.2. the Provider does not perform the service support in accordance with this Contract and/or significantly neglects to perform its obligations,

17.1.3. the Customer is in default with the payment of an invoice for more than 3 months.

17.2 The Customer is further entitled to withdraw from this Contract in the event of a significant change in control of the Provider or a change in control of the principal assets used by the Provider for performance under the Contract whereas a significant change in control means a change in the controlling entity pursuant to Section 74 et seq. of Act No. 90/2012 Coll., on Business Companies and Cooperatives (Business Corporations Act), as amended.

17.3 Either Party shall be entitled to terminate this Contract if the other Party is bankrupt as defined in its national law.

17.4 In the event of termination of this Contract by either Party according to Article 17.1 of this Contract, the termination shall be effective after the expiration of the period stated in Article 17.1 of this Contract in vain. In the event of termination of this Contract by either Party according to Article 17.2 or 17.3 of this Contract, the termination shall be effective upon delivery of a written notice to the other Party.

17.5 Either Party is entitled to terminate this Contract without giving a reason. Termination must be notified in written to the other Party. In such a case the force and effect of the Contract shall expire 3 (three) months upon the delivery of the written notice to the other Party.

17.6 This Contract may be terminated by mutual written agreement of both Parties.

17.7 In case of the contract termination, any claims of both Parties shall be settled so as to avoid any undue enrichment for either Party, the Parties will try to establish by mutual agreement a liquidation settlement; failure such an agreement, provisions of Article 14 of this Contract shall apply.

18. Penalties

18.1 In the event of a breach of the rules for VPN access pursuant to Article 8.3 of this Contract, the Provider shall pay the Customer a contractual penalty of 200 $ (in words: two hundred United States dollars) for each individual breach.

18.2 In the event of breach of duty of confidentiality according to Article 8.7 of this Contract, the breaching Party shall pay the other Party a contractual penalty of 1000 $ (in words: one thousand United States dollars) for each individual breach.

18.3 If the Provider breaches the conditions of security of the workstation set forth in the Security Rules notified pursuant to Article 4 of Annex 1 of the Contract, the Customer is entitled to demand a contractual penalty of 500 $ (in words: five hundred United States dollars) for each individual breach.

18.4 If the Provider breaches the reporting obligation in the field of security incidents/incidents set out in the Security Rules notified pursuant to Article 4 of the Annex 1 of this Contract, the Customer is entitled to demand a contractual penalty in the amount of 500 $ (in words: five hundred United States dollars) for each individual case of breach.

18.5 If the Provider fails to ensure the implementation of remedial measures resulting from the Customer's audit performed according to the conditions described in Article 8 of Annex 1 of the Contract and further specified in the Security Rules notified pursuant to Article 4 of Annex 1 of the Contract, the Customer is entitled to demand a contractual penalty of 1000 $ (in words: one thousand United States dollars) for each individual infringement.

18.6 Any penalties shall be paid by the Provider independent of the possible damage caused to the Customer, such indemnity mentioned herewith shall be the subject of separate reimbursement.

19. Miscellaneous

19.1 If any of the provisions of this Contract is found, by a competent authority, to be void or unenforceable, such provision shall be deemed to be deleted from this Contract, while the other provisions of this Contract shall remain in full force and effect. The Parties shall negotiate in good faith in order to agree upon a mutually satisfactory provision to be substituted for the provision so found to be void or unenforceable.

19.2 By signing this Contract the Provider acknowledges that it is not authorized to disclose or disseminate any information which could affect the security of civil aviation, namely due to requirements for maintaining security in civil aviation resulting from the relevant legislation (in particular the Aviation Regulation L17) and imposing on air navigation service providers to take appropriate actions as a base to provide safeguarding of civil aviation against acts of unlawful interference. Particularly, the Provider shall not anyhow reproduce and redistribute any information acquired in connection with the performance thereof.

19.3 Personal data protection

The Customer and the Provider shall comply with personal data protection rules pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), i.e. GDPR Regulation, and pursuant to other generally binding legal regulations on personal data protection. More information on data protection on the part of the Customer is available on

https://www.ans.cz/categorysb?CatCode=A6

19.4 Publication

The Provider acknowledges that the Customer is bound to publish this Contract pursuant to Act No. 340/2015 Coll., on special conditions of effect of some contracts, publishing of those contracts and the register of contracts (the Contracts Register Act), as amended. The Provider further acknowledges that the Customer is bound to provide information according to Act No. 106/1999 Coll., on free access to information, as amended. When publishing this Contract in the Register of contracts, in particular the following details shall be made illegible in its text: Provider’s bank details in Article 1 of this Contract, name of the person signing the Contract on behalf of the Customer in Article 1 of this Contract and in the signature part, Provider´s email address in Article 6.5 of this Contract, contact details stated in Article 15.1 of this Contract, signatures on the Contract and trade secret within the sense of § 504 Civil Code as further specified in Article 19.5 of this Contract.

19.5 Trade secret

Trade secret, within the sense of § 504 of the Civil Code, means the price calculation as stated in Articles 6.1.1 and 6.1.2 of this Contract and for this reason will neither be published nor provided according to Article 19.4 of this Contract.

20. Final provisions

20.1 Both Parties declare that the individual Articles of this Contract are sufficient with regards to the requirements for forming a contractual relationship, that the contractual freedom of the Parties has been used and that the Contract has been concluded in such a way that it is not to the debit of either Party.

20.2 This Contract shall not be modified or amended, except by written amendment signed by the authorized representatives of the Parties.

20.3 Both Parties declare that, regarding their own national regulations, they are fully entitled to sign the present Contract.

20.4 This Contract shall be valid upon signature by the Customer and the Provider, and shall be effective from 1st March 2024 on the condition that the publication of the Contract in the Register of contracts precedes such date. If the Contract is published in the Register of contracts after 1st March 2024, it shall be effective from the date of its publication in the Register of contracts.

20.5 **This Contract has been signed electronically, only in one electronic copy.**

20.6 The Annex below make an integral part of this Contract:

Annex 1 Cyber security measures

[redacted]

Annex 1 – Cyber Security

Contractual ensuring of measures in the area of information and cybersecurity within the meaning of Section 8 (2) of the Regulation No. 82/2018 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 major contractor according to Section 2 (n) of the Cybersecurity Regulation for the Customer, which is Air Navigation Services of the Czech Republic (ANS CR), 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 major contractor relates to: Surface Movement Radar SR-03.

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 4 hereof.

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.

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 Provider according to the Contract who is also a major contractor according to Section 2 (n) of the Cybersecurity 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 according to this Annex as required for ensuring of security of the information/communication systems referred to in Article 1.2 hereof and maintain appropriate security documentation.

3.2 The Security Measures set out in in this Annex shall be set in line 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 the CSN ISO/IEC 27001 standard.

3.3 The Customer shall verify the implementation and realisation of the Security Measures in compliance with Article 8 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.

4. Adherence to Customer's Security Policies

4.1 The Provider shall comply with the "Security Rules for Major Contractors" of the Customer that are available at the following websites:

https://www.ans.cz/content/documents/Security_rules_for_major_contractors.pdf

with exception of the articles 7.1.2, 8, 11 and 12.1.3 that are not binding for the Provider.

(hereinafter referred to as the "**Security Rules**"). The Provider hereby confirms that he got to know the Security Rules and agrees with them.

4.2 The Customer is obliged, via the cyber security manager, to provide the Provider with Security Rules supplemented with details of Customers security standards within 10 days from the effectiveness of the Contract. Such supplemented Security Rules shall be distributed by electronically signed e-mails.

4.3 The Customer may, in connection with legislative changes, decisions or warnings from the National Cyber and Information Security Agency, decisions of other administrative authorities and/or fulfilment of remedial measures resulting from state supervision, after Contract signature change the Security Rules from time to time. The amended Security Rules shall be distributed in electronic (digital) form, meaning email with attachments converted in pdf format and signed by Cyber Security manager with recognized electronic signature (in accordance with eIDAS), databox or in the form of letter signed by Cyber Security manager sent via the holder of postal licence with confirmation of delivery on the address of Provider`s Cyber Security Manager. In case the Provider does not disagree with the amended Security Rules within 10 working days from the delivery of its announcement, it is considered to agree with amendment and the Provider shall comply with such amended Security Rules.

4.4 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 Security Rules.

5. Change Management

5.1 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 8 hereof, the Provider is required to document the risk management method.

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

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

5.4 The Provider 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. The Provider shall ensure such cooperation also with his subcontractors.

5.5 If, within its solution required for provision of the services under the Contract, the Provider makes use of technical or programme tools of Huawei Technologies Co., Ltd. or ZTE Corporation including their subsidiaries, the Provider within the tender process submitted to the Customer a risk analysis prepared in compliance with the methodology of the National Cyber and Information Security Agency (NÚKIB).

6. **Notification Requirements**

6.1 The Provider shall inform the Customer without undue delay via the Cybersecurity manager, 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.

6.2 The Provider shall use Customer´s Cybersecurity manager contact 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.

6.3 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 whereas a significant change in control means a change in the controlling entity pursuant to Section 74 et seq. of Act No. 90/2012 Coll., on Business Companies and Cooperatives (Business Corporations Act), as amended.

6.4 More detailed conditions of reporting and classification of security incidents are specified in the Security rules.

7. **Subcontractors**

7.1 In accordance with Section 105 (4) in conjunction with Section 3 of Act No. 134/2016 Coll., On Public Procurement, as amended, according to Czech law, 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 Customer prior to commencement of performance by the subcontractor concerned.

7.2 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.

7.3 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 in the Contract and are meeting the requirements of the applicable legislation relating to contractual performance;

c) provide the Customer at its request with copies of selected parts of contracts with subcontractors (or similar documents) relevant for performance of the Contract;

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

7.4 In case that the Security Rules form an integral part of an agreement with subcontractors or between subcontractors, the Provider shall inform the Customer in advance. The Customer 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 Customer finds this need justified or fails to assess the new subcontractor as a security risk, the Customer will allow to provide this safety information to the specific subcontractor.

8. Inspections and quality control

8.1 If requested, the Provider and all subcontractors shall provide access to all information required for proving of compliance herewith and cooperate during audits and inspections conducted by any auditor authorized by the Customer. The Provider shall ensure such cooperation also on the part of the subcontractor, if applicable.

8.2 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 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).

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