Public Contract for the Provision of National CERT Activities and for Cooperation in the Field of Cyber Security

pursuant to Section 19 of Act No. 181/2014 Coll., on Cyber Security, and Section 159 et seq. of Act No. 500/2004 Coll., the Administrative Procedure Code, as amended (hereinafter the "Administrative Procedure Code")

(hereinafter the "**Contract**")

Czech Republic - National Security Authority

Seat: Na Popelce 2/16, 150 06 Prague 5
Company ID No.: 68403569
Data box ID: h93aayw
Ref. No.: 9625/2015-NBÚ/41
Represented by Ing. Dušan Navrátil, director of the National Security Authority
(hereinafter the "**NSA**")

and

CZ.NIC, z.s.p.o.

Seat: Milešovská 1136/5, 130 00 Prague 3 - Vinohrady
Company ID No.: 67985726
Data box ID: h4axdn8
Represented by Mgr. Ondřej Filip, MBA, under power of attorney dated 22 May 2015
(hereinafter "**CZ.NIC**")

(the NSA and CZ.NIC shall hereinafter be jointly referred to as the "**Parties**")

WHEREAS

A. Under Section 22 of Act No. 181/2014 Coll., on Cyber Security (hereinafter the "Cyber Security Act"), the NSA performs state administration in the field of cyber security, and the Cyber Security Act embodies the functioning of two primary supervisory departments, to which the Act gives competences in the field of cyber security in the Czech Republic, and one of which is National CERT;

B. On 15 April 2015, in accordance with Section 19(1) of the Cyber Security Act, the NSA announced a procedure for the selection of an application for the conclusion of a public contract for the purpose of cooperation in the field of cyber security and the provision of the activities of National CERT pursuant to Section 17(2) of the Cyber Security Act; on 17 August 2015, the NSA selected the application of CZ.NIC, z.s.p.o.;

C. CZ.NIC is a special-interest association of legal entities associating significant legal entities operating in the Czech Republic in the area of domain names and in the electronic communications market which operates the top-level domestic domain .cz (ccTLD .cz) and is engaged, among other things, in the area of Internet security and computer and cyber security, and operates the CSIRT.CZ security team;

D. Before the conclusion of this Contract, the role of National CERT was performed by the CSIRT.CZ security team operated by CZ.NIC under the Memorandum of CERT/CSIRT of the Czech Republic dated 19 December 2012;

NOW, THEREFORE, THE PARTIES ENTER INTO THIS CONTRACT ON THE DAY, MONTH AND YEAR SET FORTH BELOW:

PART I

Opening Provisions

ARTICLE I

Subject-Matter of the Contract

1. On the basis of this Contract, CZ.NIC undertakes to operate National CERT under the conditions laid down in the Cyber Security Act and this Contract.
2. CZ.NIC and the NSA further undertake to develop cooperation in the field of cyber security in order to achieve the maximum possible degree of cyber security of the Czech Republic (hereinafter the "**Cooperation**").
3. For the purpose of ensuring the proper performance of the subject-matter of the Contract throughout its term, CZ.NIC undertakes to achieve a sufficient organisational and institutional capacity and financial stability and to have sufficient technical and technological resources at least at the level indicated in the "Application for the Conclusion of the Public Contract for Cooperation in the Field of Cyber Security and for the Provision of the Operation of the National Security Team" (hereinafter the "**Application**"), with which CZ.NIC participated in the procedure for the selection of an application for the conclusion of a public contract with the NSA for the purpose of cooperation in the field of cyber security and the provision of activities pursuant to Section 17(2) of the Cyber Security Act - selection of the National CERT operator, announced under ref. No. 2688/2015-NBÚ/80 on 15 April 2015, and which is attached as Schedule 1 hereto.
4. Under this Contract, written **Implementing Protocols**, numbered in ascending order, will be made to specify the conditions for the operation of National CERT and to provide a detailed regulation of the mutual Cooperation.

On behalf of the NSA, the Implementing Protocols will be signed by:

- Deputy Director of the Cyber Security Department, or

- Director of the National Cyber Security Centre.

As of the date of this Contract, Ing. Jaroslav Šmíd is the Deputy Director of the Cyber Security Department and Mgr. Vladimír Rohel is the Director of the National Cyber Security Centre.

On behalf of CZ.NIC, the Implementing Protocols will be signed by:

- The Board of Directors, or
- The Executive Director of CZ.NIC

As of the date of this Contract, Mgr. Ondřej Filip, MBA is the Executive Director of CZ.NIC.

No future change in the persons authorised to sign the Implementing Protocols shall constitute a reason to amend this Contract; such a change in the persons authorised to sign the Implementing Protocols will be notified to the other Party through the data box information system (hereinafter the "ISDS") if permitted by the nature of the Parties' data boxes.

PART II
Operation of National CERT

ARTICLE II
Rights and Obligations of CZ.NIC in the Operation of National CERT

1. CZ.NIC is committed to the proper operation of National CERT in accordance with the best practice of CERT/CSIRT teams and other national and international standards, particularly in the field of cyber security. The surveillance centre - National CERT - will be operated by the CSIRT.CZ security team run by CZ.NIC. CZ.NIC agrees to operate National CERT through the CSIRT.CZ security team on its own responsibility.
2. CZ.NIC undertakes to apply itself to the prevention of cyber attacks to a reasonable extent, for example through the operation of passive detection tools, or if necessary through an active search for vulnerable or inadvisedly configured devices available especially via the Internet.
3. CZ.NIC undertakes to keep the CSIRT.CZ security team membership in multinational organisations operating in the field of cyber security, especially those that were indicated in the Application.
4. CZ.NIC hereby agrees that
   a) It will be authorised to access classified information of the Restricted classification level pursuant to Act No. 412/2005 Coll., on Protection of Classified Information and Security Capacity, as amended (hereinafter the "Classified Information Protection Act"), under the declaration of an entrepreneur pursuant to Section 15a of the Classified Information Protection Act or under a valid certificate of an entrepreneur of the Confidential, Secret or Top Secret classification level, at least for the form of access under Section 20b) of the Classified Information Protection Act, and
   b) Individuals whose activities require access to classified information in the performance of the subject-matter of the Contract, i.e. the Executive Director, the Operations Manager and analysts, will hold valid personal certificates for access to classified information of the Confidential classification level,

or a notice of compliance with the conditions for access to classified information of the Restricted classification level within the meaning of the Classified Information Protection Act.

5. CZ.NIC agrees to publish regular reports on the activities of National CERT once a year, but no later than the end of March of the following calendar year. By the end of February, CZ.NIC shall submit a report for commenting by the NSA; the NSA shall submit the comments on the report to CZ.NIC within 14 days of the receipt of the report. The information in the report will form one of the bases for the preparation of the Report on the State of Cyber Security of the Czech Republic, which is prepared and submitted to the Government of the Czech Republic by the NSA annually; the NSA shall send the Report to CZ.NIC for commenting at least 1 month prior to the submission thereof to the Government of the Czech Republic.

6. In accordance with the Application, CZ.NIC agrees to maintain an information security management system at the level of the ČSN ISO/IEC 27001 standard or a similar recognised standard ensuring the protection of information at the same or a better level. The NSA reserves the right to require the submission of the report on the last conducted surveillance/recertification audit proving the compliance with the aforesaid standard within 30 days of the delivery of the NSA's request.

7. In accordance with Section 17(3) of the Cyber Security Act, CZ.NIC is authorised to perform other activities in the field of cyber security not governed by the Cyber Security Act, in its own name and on its own responsibility, including economic activities, provided that such other activities do not interfere with the fulfilment of the obligations set out in Section 17(2) of the Cyber Security Act.

8. In the case of a reasonable suspicion that CZ.NIC does not comply with the conditions stipulated by the law and the Contract in the performance of the activities of National CERT, the NSA shall be entitled to request CZ.NIC to submit the report on the last conducted surveillance/recertification audit pursuant to the ČSN ISO/IEC 27001 standard or a similar recognised standard ensuring the protection of information at the same or a better level, within 30 days of the delivery of the NSA's request. If CZ.NIC fails to submit that report, the NSA shall be authorised to check the performance of the activities of National CERT pursuant to Section 23 of the Cyber Security Act.

ARTICLE III
Statutory Duties of National CERT

1) In accordance with Section 17(2)a) of the Cyber Security Act, National CERT will receive contact data from the bodies and persons referred to in Section 3a) and Section 3b) of the Cyber Security Act, and will record and archive these data. CZ.NIC as the National CERT operator will also enable receiving these contact data through the ISDS. For this purpose, the NSA agrees that CZ.NIC may dispose of a public authority data box, in accordance with Section 5a of Act No. 300/2008 Coll., on Electronic Acts and Authorised Document Conversion.

2) In accordance with Section 17(2)b) of the Cyber Security Act, National CERT will receive reports of cyber security incidents from the bodies and persons referred to in Section 3b) of the Cyber Security Act, and will record, archive and protect these data, while

   a) CZ.NIC undertakes to establish and maintain a surveillance centre and customer support with non-stop operation performing the role of the last resort, through which the bodies and persons referred to in Section 3b) of the Cyber Security Act will report cyber security incidents to National CERT, and

b) National CERT is authorised to receive reports of cyber security events and cyber security incidents from other entities as well; National CERT will provide assistance in addressing such events and incidents to a reasonable extent and only if it has a sufficient capacity for it, and National CERT is not obliged to provide support and assistance to end users.

3) In accordance with Section 17(2)c) of the Cyber Security Act, National CERT will evaluate cyber security incidents at the bodies and persons referred to in Section 3b) of the Cyber Security Act,

4) In accordance with Section 17(2)d) of the Cyber Security Act, National CERT will provide the bodies and persons referred to in Section 3a) and Section 3b) of the Cyber Security Act with methodological support, assistance and cooperation in the event of a cyber security incident. Assistance shall mostly mean coordination and methodological assistance. National CERT is not obliged to provide physical resources.

5) In accordance with Section 17(2)e) of the Cyber Security Act, National CERT will act as a contact point for the bodies and persons referred to in Section 3a) and Section 3b) of the Cyber Security Act,

6) In accordance with Section 17(2)f) of the Cyber Security Act, National CERT will conduct assessments of vulnerabilities in the field of cyber security,

7) In accordance with Section 17(2)g) of the Cyber Security Act, National CERT will provide the NSA with data on cyber security incidents without the name of the reporter of the cyber security incident. The scope of the data and the method of provision will be established through the Implementing Protocol.

8) In accordance with Section 17(2)h) of the Cyber Security Act, National CERT will, at the request of the NSA, provide the NSA with the contact details of the bodies and persons referred to in Section 3a) and Section 3b) of the Cyber Security Act in the event of a cyber danger. National CERT is obliged to provide these details to the NSA immediately upon the request.

9) In the performance of the duties of National CERT under par. 1-8, CZ.NIC is obliged to act impartially in accordance with Section 17(5) of the Cyber Security Act; in accordance with Section 17(4) of the Cyber Security Act, CZ.NIC is obliged to coordinate its activities with the NSA in the performance of these duties, especially where such a cooperation is required by circumstances which have a significant impact on the cyber security of the Czech Republic, i.e. mainly in cases of declared cyber danger pursuant to Section 21 of the Cyber Security Act and other crisis situations caused in particular by a major breach of the cyber security of the Czech Republic.

10) If, in the course of dealing with the cyber security incident by National CERT, a situation arises that has or may have a significant security impact on a crucial information infrastructure, a major information system or a public administration information system, and if CZ.NIC, given its awareness of the information available, can be reasonably expected to identify such a significant security impact, National CERT shall immediately forward this information to the NSA and proceed in coordination with the NSA in addressing the incident.

11) National CERT will collect and analyse data on cyber security events, cyber security incidents and other cyber security threats of which National CERT learns in the course of its activities. It will forward such information to the NSA and other entities operating in the field of cyber security in accordance with the arrangements set out in Article IV.

ARTICLE IV
Exchange of Information

1. National and international exchange of information on cyber threats and risks among National CERT, other CERT/CSIRT teams and other entities operating in the field of cyber security will take place depending on the sensitivity of the information and the seriousness of the situation in accordance with the existing legal regulations, the best practice of the CERT/CSIRT teams and other national and international standards, particularly in the field of cyber security (such as the Traffic Light Protocol – TLP), in order to prevent misuse of such information. This shall be without prejudice to the provisions of Article III(7).
2. In accordance with Section 9(4) of the Cyber Security Act, the NSA will provide data from the incident records of CZ.NIC to the extent necessary to ensure the protection of cyberspace, according to the seriousness of the findings and the state of the cyber security incident, and in accordance with the principle of proportionality in relation to the seriousness of the content of the data provided.
3. CZ.NIC undertakes to protect and prevent the misuse of the data obtained in connection with the activities referred to in Section 17(2) of the Cyber Security Act. CZ.NIC in particular undertakes not to provide these data to third parties except in cases of sharing information as set forth herein, and not to provide or use these data for commercial purposes. This obligation shall continue after the termination of the Contract, and the provisions of Article VIII(2) hereof shall apply by analogy.
4. CZ.NIC agrees to regularly publish updated information and statistics on the number and types of cyber security incidents addressed on the National CERT website operated by CZ.NIC.
5. The Parties will determine the technical details and the manner of information exchange through the Implementing Protocols.

ARTICLE V
Financing the Operation of National CERT

1. The costs associated with the operation of National CERT shall be borne by CZ.NIC.
2. CZ.NIC will perform the duties under Article III(1), (2), (3), (5), (7) and (8) hereof without charge.
3. CZ.NIC is entitled to demand financial compensation from third parties for the performance of activities referred to in Article III(4) and (6) hereof, and also for the performance of other economic activities in the field of cyber security pursuant to Section 17(3) of the Cyber Security Act.
4. CZ.NIC may apply for aid for the financing of the operation of National CERT from private, departmental, governmental or international sources, especially in the form of grants or from funds.
5. The NSA shall support CZ.NIC in obtaining the funds for financing the activities of National CERT hereunder, especially from national and international sources in the form of grants or from

funds, unless this may be seen as a conflict of interest with respect to the involvement of the NSA in the bodies that make decisions as regards the provision of such funds.

6. The NSA is entitled to request, annually, that CZ.NIC prove financial stability and the ability to maintain proper operation of National CERT.

PART III
Cooperation

ARTICLE VI
Content of Cooperation

1. The Cooperation includes in particular:

   a) Expert assistance of CZ.NIC in inspections in the field of cyber security carried out by the NSA pursuant to Section 23 of the Cyber Security Act, and also in forensic activities; for this purpose, CZ.NIC will provide the NSA with human and technical resources upon previous agreement,

   b) Education and raising awareness in the field of cyber security in the form of workshops, lectures, conferences, trainings, events relating to this field and the publication of electronic and printed materials concerning these topics; the Parties will inform each other of the planned activities sufficiently in advance, and will coordinate the preparation of such activities,

   c) Development of cooperation with third parties operating in particular in the field of cyber security at the national and international levels, where the Parties will coordinate their positions and work together to promote and ensure a single image of the cyber security of the Czech Republic within the international organisations in which they are members, by participating in events in the Czech Republic and abroad and through mutual support and the promotion of their activities in this area,

   d) Cooperation in the establishment of other CERT/CSIRT teams in the Czech Republic, where both parties shall promote the formation of new cyber security teams at academic institutions and private corporations,

   e) Exchange of experience, knowledge, know-how and information in particular in the field of cyber security, where the Parties agree to provide each other with the results of the research projects, tasks and solutions that they conduct or in which they participate, to the largest extent possible; unless the Party that provides such data determines otherwise, these results will be available through the NSA to all entities working on the protection of cyberspace, including public administration bodies, operators of crucial information infrastructures, bodies or persons securing major networks, and administrators of major information systems,

   f) Joint participation in cyber security and defence trainings; at the request of the NSA, upon mutual agreement, CZ.NIC will take part in national and international trainings and other events related to the operation of National CERT and the cyber security of the Czech Republic, and the NSA will invite CZ.NIC to attend such events,

   g) Cooperation in the preparation of bills and related documents in the field of cyber security,

   h) Further cooperation depending on the current need for activities to ensure the cyber security of the Czech Republic.

2. At the request of the NSA, CZ.NIC will attend the meetings of the Cyber Security Council and the meetings of the working bodies set up by the NSA in dealing with major cyber security incidents that may have a significant security impact on the cyber security of the Czech Republic, unless the attendance of CZ.NIC is ruled out for serious reasons in a particular case. CZ.NIC will provide the NSA with the contact data of the persons who will represent CZ.NIC in fulfilling this duty and who meet the requirements for accessing classified information to which they may have access in this context, at least at the classification level necessary to participate in the given meeting. In the case of discussing classified information of a higher level of classification, the NSA shall take the necessary measures to prevent unauthorised access to that information. In the event CZ.NIC is absent from a meeting of the Cyber Security Council or a meeting of the working bodies set up by the NSA in dealing with major cyber security incidents, the NSA is obliged to inform CZ.NIC of the outcomes of such a meeting if the outcomes may affect the activities of National CERT hereunder.
3. The conditions of the Cooperation will be determined by the Parties in more detail in the form of the Implementing Protocols, including the financial security of the specific Cooperation if agreed upon by the Parties in writing. The Parties may also continuously develop the Cooperation in an informal way.
4. The Cooperation between CZ.NIC and the NSA will be provided by CZ.NIC in a scope consistent with the capacity, personnel, time and financial possibilities of CZ.NIC.

PART IV
Miscellaneous Provisions

ARTICLE VII
Intellectual Property Rights

1. Throughout the performance of this Contract, the Parties undertake to honour and protect industrial rights, intellectual property rights, copyright and trade secrets.
2. If, in the performance of the subject-matter of the Contract, a work is created by the activities of the Parties and such a work has the characteristics of a copyrighted work under Act No. 121/2000 Coll., the Copyright Act, as amended, especially as a result of research and development or educational activities in the field of cyber security, the Parties may determine the conditions for granting the right to use such a work in the form of an Implementing Protocol.

ARTICLE VIII
Confidentiality

1. The Parties are obliged to maintain confidentiality with respect to
   a) Information in the cases as set out in the existing legal regulations and other national and international standards, particularly in the field of cyber security (such as the Traffic Light Protocol – TLP),
   b) Data on cyber security incidents recorded in accordance with the Cyber Security Act, with the exception of data that are to be made public under this Contract or the Cyber Security Act, and

c) Information which the Parties learn upon entering into the Contract or during the term hereof in the exercise of the rights and the performance of the duties arising from the Contract; this shall mean any information in verbal or written form as well as know-how that is deemed to comprise all knowledge of commercial, manufacturing, security, technical or economic nature including software and documentation, relating to the activities of one of the Parties, which has real or at least potential value and which is not readily available, and the respective Party has expressed the wish that the confidentiality obligation apply to this information, or such a wish may be reasonably assumed given the nature of the information.

2. The Parties undertake not to disclose the information under this Article to any third party and to take such measures as to prevent the disclosure of the information to third parties. The provisions of the previous sentence shall not apply under the following circumstances
   a) The Parties are required to provide the information by the law,
   b) The Parties provide information to third parties or publish information under this Contract,
   c) Such information becomes a matter of public domain or available otherwise than as a consequence of a breach of obligations by one of the Parties; or
   d) The other Party gives its consent to making a specific piece of information available.
3. If either Party gains access to personal data within the meaning of Act No. 101/2000 Coll., on Personal Data Protection, as amended, in the exercise of the rights and the performance of the duties arising from the Contract, that Party is obliged to ensure disposal of such data in accordance with that Act, and shall be liable for any damage caused to the other Party or third parties in the event of breach of this obligation.
4. The obligations under par. 1-3 shall survive the termination of the Contract.
5. The Parties agree that the confidentiality obligation shall not apply to the information on the conclusion of this Contract and the content hereof, with the exception of the Implementing Protocols that will contain classified information or will be marked as private, and the Parties may make the information on the conclusion of this Contract and the content hereof public, even in a manner enabling remote access.
6. The Parties agree that information on the activities of National CERT under this Contract and the Cyber Security Act will be provided by the NSA according to the legislation on free access to information. CZ.NIC is obliged to provide the NSA with the assistance necessary for that purpose.

ARTICLE IX
Term and Termination of the Contract

1. In accordance with Section 164(2) of the Administrative Procedure Code, the Contract shall enter into force and effect upon its signing by the last Party if both Parties are present. If the Parties are not present at the same time, the Contract shall be deemed made upon the receipt

of the draft signed by the other persons to whom it was intended by the person who drafted the Contract.

2. The Contract is entered into for an indefinite period.
3. The Contract may be terminated
   a) Based on a written agreement between the Parties;
   b) By written notice of either Party without the need to give a reason. The notice period shall be 6 months commencing on the first day of the month following the month in which the notice was delivered to the other Party;
   c) By withdrawal from the Contract in the event the other Party substantially breaches the Contract and fails to remedy the situation within a reasonable period allowed by the other Party. The withdrawal must be made in writing, otherwise it shall be deemed invalid; the withdrawal shall become effective upon its receipt by the other Party. A substantial breach of the Contract includes in particular the following:
      i. Breach of the confidentiality obligation laid down in Article VIII hereof, in particular in the form of an unauthorised disclosure, the misuse of information for commercial or other purposes, or an insufficient protection of information that causes or may cause an extensive information leakage,
      ii. Failure of CZ.NIC to ensure the necessary organisational and institutional capacity, financial stability, and technical and technological resources for the purposes of performing the subject-matter of the Contract,
      iii. Failure of CZ.NIC to comply with other requirements for the operation of National CERT set out in Section 18(2) of the Cyber Security Act,
      iv. Breach of the obligation to operate National CERT impartially,
      v. Breach of the obligation laid down in Article II(7) of the Contract,
      vi. Repeated failure to invite CZ.NIC to attend or a repeated absence of CZ.NIC at the meetings of the Cyber Security Council or at the meetings of the working bodies set up by the NSA in dealing with major cyber security incidents that may have a significant impact on the cyber security of the Czech Republic,
      vii. Failure to provide information on the outcomes of meetings that may have a significant impact on the activities of the other Party in the event that Party was not invited to such meetings.
   d) By a written proposal of either Party for the cancellation of the Contract within the meaning of Section 167(1) of the Administrative Procedure Code. If the other Party consents to the proposal, the Contract shall terminate as of the date on which the written consent is delivered to the Party which submitted the proposal. If the other Party does not consent to the cancellation of the Contract, the administrative body

competent under Section 169(1) of the Administrative Procedure Code may decide on the cancellation of the Contract at the request of the Party which submitted the proposal. Either Party may submit a proposal for the Contract cancellation:

i. If the situation which was decisive for determining the content of the Contract changes substantially, and the Party cannot be reasonably required to perform the Contract for that reason,

ii. If the Contract comes into conflict with the law,

iii. By reason of the protection of the public interest, or

iv. If facts that existed at the time of entering into the Contract and that were not known to the Party with no fault of that Party come to light, and the Party proves that it would not have entered into the Contract if it had known those facts.

4. As of the date of termination of the Contract, CZ.NIC is obliged to give to the NSA in writing (i.e. in electronic machine-readable form) all contact details, records of cyber security event and incident reports, and the outcomes of other activities and Cooperation created or obtained in connection with the operation of National CERT.

ARTICLE X
Final Provisions

1. The legal relations not expressly regulated by the Contract and arising from the Contract or related to it shall be governed by the relevant provisions of Act No. 500/2004 Coll., the Administrative Procedure Code, as amended, and by the relevant provisions of Act No. 89/2012 Coll., the Civil Code.
2. If the Contract requires written form in the case of a certain act of a Party, the notification of such an act shall be delivered to the other Party via the ISDS if permitted by the nature of the Parties' data boxes, or by registered letter, by courier or in person against a signature to the address of the seat of the other Party indicated in the heading of the Contract. If the Party refuses to accept the notification of the act of the other Party, the notification shall be deemed delivered on the day of such a refusal. In the event the notification is sent by post, it shall be deemed delivered on the third day after handing the notification over to the postal service.
3. Any changes or supplements to the Contract may only be made in the form of written amendments numbered in ascending order, signed by the authorised representatives of the Parties. The Implementing Protocols may only be modified in writing.
4. In the case of any disagreements or disputes between the Parties, the Parties undertake to make every effort to find an amicable solution.
5. Should any provision of this Contract become invalid or ineffective due to changes in legislation, this shall be without prejudice to the validity or effectiveness of any other provisions herein. In such a case, the Parties undertake to make every effort to conclude an amendment to the Contract that will replace the invalid or ineffective provision with a new provision the content

of which will be as close as possible to the original will of the Parties and which will be in accordance with the existing legal regulations. Until the conclusion of the amendment, the relationship between the Parties in that matter shall be governed by generally binding legislation.

6. The Contract is drawn up in four (4) counterparts, each considered an original document, of which each Party shall obtain two upon the signing thereof. The Contract will also be published in the NSA Journal in accordance with Section 19(3) of the Cyber Security Act.

7. The Parties declare that the Contract was made on the basis of their true and free will, that the Parties read the Contract prior to its signing, and that they agree to the entire content hereof, in witness whereof the Parties attach their handwritten signatures below.

8. The following Schedules form an integral part of this Contract:

   Schedule 1 to the Contract - Application for the Conclusion of the Public Contract for Cooperation in the Field of Cyber Security and for the Provision of the Operation of the National Security Team

In Prague, on	In Prague, on
National Security Authority:	CZ.NIC, z.s.p.o.:
.....	.....

Schedule 1 to the Contract

Application for the Conclusion of the Public Contract for Cooperation in the Field of Cyber Security and for the Provision of the Operation of the National Security Team