Data Security Agreement	Zmluva o bezpečnosti údajov

Contractor / Dodávateľ		University Hospital Trnava ("Institution") / Fakultná nemocnica Trnava („inštitúcia")	
Full Trade Name / Celý obchodný názov	iSchemaView, Inc.	Full Name / Celý názov	Fakultná nemocnica Trnava
Details of Company Incorporation / Údaje o založení spoločnosti	Delaware Corporation	Details of Establishment / Údaje o zriadení	Zriaďovacia listina Ministerstva zdravotníctva Slovenskej republiky č. 1970/1991-A/IV-1 zo 14. júna 1992 v znení neskorších rozhodnutí
Company Address / Adresa spoločnosti	405 El Camino Real Suite 601, Menlo Park, CA 94025 USA	Phone Number / Telefón	Andreja Žarnova 11, Trnava, 917 75, Slovensko

Article I
INTRODUCTORY PROVISIONS

1. Institution is the Operator of Essential Services under the Cybersecurity Act of the Slovak Republic No. 69/2018 (the "**Cybersecurity Act**").
2. The identified essential services provided by the Operator of Essential Services are generally:
   a) Public administration information systems.
   b) Hospital information system.
   c) Laboratory information systems.
3. The Institution enters into the SOFTWARE SUPPLY AND LICENSE AGREEMENT with an effective date of ..... }{DATE} (the "**Main Agreement**") with the company A care, Hraničná 5, Trebatice 922 10, IČO: 35724609, the subject matter of which affects or is directly related to the operation of networks and information systems as defined in the Cybersecurity Act for the Operator of Essential Services. The subject of the Main Agreement is the provision of RAPID software, which is a platform enabling an expert software solution aimed at estimating disability and subsequent treatment of brain tissue in neurovascular diseases, of which Contractor is the author.

Article II
BASIC TERMS

For the purposes hereof:

a) Contract refers to this Data Security Agreement.
b) network and information system refer to an

Článok I
ÚVODNÉ USTANOVENIA

1. Inštitúcia je Prevádzkovateľom základných služieb podľa zákona Slovenskej republiky č. 69/2018 o kybernetickej bezpečnosti (ďalej len „**zákon o kybernetickej bezpečnosti**").
2. Identifikované základné služby poskytované Prevádzkovateľom základných služieb sú vo všeobecnosti:
   a) informačné systémy verejnej správy;
   b) nemocničný informačný systém;
   c) laboratórne informačné systémy.
3. Inštitúcia uzatvára ZMLUVU NA DODÁVKU SOFTVÉROVÉHO DIELA A UDELENIE LICENCIE NAŇ s dátumom účinnosti }{DÁTUM} (ďalej len „**Hlavná zmluva**") so spoločnosťou A care, Hraničná 5, Trebatice 922 10, IČO: 35724609, ktorej predmet sa dotýka alebo priamo súvisí s prevádzkou sietí a informačných systémov v zmysle zákona o kybernetickej bezpečnosti pre Prevádzkovateľa základných služieb. Predmetom Hlavnej zmluvy je dodanie softvéru RAPID, ktorý predstavuje platformu umožňujúcu expertné softvérové riešenie zamerané na odhad postihnutia a následnú liečbu mozgového tkaniva pri neurovaskulárnych ochoreniach, ktorého je Dodávateľ autorom.

Článok II
ZÁKLADNÉ POJMY

Na účely tejto zmluvy:

a) Zmluva označuje túto Zmluvu o bezpečnosti údajov;

electronic communications network, an information system, any equipment and communication system or the data generated, stored, processed, retrieved or transmitted thereon by means of an electronic communications network or information system, for the purpose of operating, using, protecting and maintaining those networks and systems; c) cyberspace refers to the global dynamic open system of networks and information systems, consisting of the activated cyberspace elements, the persons carrying out activities in that system, and the relationships and interactions between them; d) continuity refers to the strategic and tactical ability of an organisation to plan for and respond to events and incidents in order to continue to perform activities at an acceptable, predefined level; e) confidentiality refers to the guarantee that data or information is not disclosed to unauthorised entities or processes; f) availability refers to the guarantee that the data or information is accessible to the user, information system, network, or device at the moment the data and information is needed and required; g) integrity refers to the guarantee that the accuracy, completeness, or correctness of the information has not been compromised; h) cybersecurity refers to the state in which networks and information systems are able to withstand, with a certain degree of reliability, any action that compromises the availability, authenticity, integrity, or confidentiality of the data stored, transmitted or processed, or related services provided or accessed through those networks and information systems; i) risk refers to a measure of cyber threat expressed in terms of the likelihood of an adverse event occurring and its consequences; j) threat refers to any reasonably identifiable circumstance or event against networks and information systems that may have a negative impact on cybersecurity; k) cybersecurity incident refers to any event which, by reason of a breach of network and information system security or a breach of security policy or binding methodology, has a negative impact on cybersecurity or results in • loss of data confidentiality, destruction of data or breach of system integrity, restriction or denial of availability of an essential service or digital service; • a high likelihood that the activities of the	b) sieť a informačný systém označujú elektronickú komunikačnú sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov; c) kybernetický priestor označuje globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi; d) kontinuita označuje strategickú a taktickú schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni; e) dôvernosť označuje záruku, že údaje alebo informácie nie sú prezradené neoprávneným subjektom alebo procesom; f) dostupnosť označuje záruku, že údaje alebo informácie sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná; g) integrita označuje záruku, že bezchybnosť, úplnosť či správnosť informácií neboli narušené; h) kybernetická bezpečnosť označuje stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov; i) riziko označuje mieru kybernetického ohrozenia vyjadrenú pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami; j) hrozba označuje akúkoľvek primerane rozpoznateľnú okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť; k) kybernetický bezpečnostný incident označuje akúkoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

essential service or digital service will be compromised; or
- a compromise of information security;

l) essential service refers to a service that is included in the list of essential services; and
- depends on networks and information systems and is an activity in at least one sector or subsector as defined in Annex 1 to the Cybersecurity Act;
- is a public administration information system; or
- is an element of critical infrastructure;

m) Operator of Essential Services refers to a public authority or a person who operates at least one of the services referred to in section k);

n) digital service refers to a service the type of which is listed in Annex 2 to the Cybersecurity Act,

o) information security manager (ISM) refers to the person in charge of information and cybersecurity management who has the powers and duties defined in the Information Security Policy and other directives of the Operator of Essential Services. These include, in particular, control activities, handling security and cyber incidents, managing the implementation of security measures, consulting and methodological activities in the field of information and cyber security, and others;

p) cybersecurity incident management refers to all procedures related to the notification, detection, analysis, and response to a cybersecurity incident and to the containment of its consequences.

Article III

SUBJECT MATTER OF THE CONTRACT

1. Under Section 19(2) of the Cybersecurity Act and with respect to the Main Agreement, the subject matter hereof is to determine the rights and obligations of the Parties in ensuring the fulfilment of security measures and notification obligations.

Article IV

OBLIGATIONS OF THE CONTRACTOR

1. The Contractor undertakes to adopt and comply with the cybersecurity measures of the Operator of Essential Services to the extent set out herein in order to meet the objectives hereof. A list of the security measures of the Operator of Essential Services and the related cybersecurity management process set-up is set out in Annex 2 hereto.

- strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby;
- vysoká pravdepodobnosť ohrozenia činností základnej služby alebo digitálnej služby alebo
- ohrozenie bezpečnosti informácií;

l) základná služba označuje službu, ktorá je uvedená v zozname základných služieb a
- závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona o kybernetickej bezpečnosti;
- je informačným systémom verejnej správy alebo
- je prvkom kritickej infraštruktúry;

m) Prevádzkovateľ základných služieb označuje orgán verejnej moci alebo osobu, ktorá prevádzkuje aspoň jednu službu podľa písmena k);

n) digitálna služba označuje službu, ktorej druh je uvedený v prílohe č. 2 zákona o kybernetickej bezpečnosti;

o) manažér informačnej bezpečnosti (ISM) označuje osobu zodpovednú za riadenie informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti vymedzené v politike informačnej bezpečnosti a v ďalších smerniciach Prevádzkovateľa základných služieb. Ide najmä o kontrolnú činnosť, riešenie bezpečnostných a kybernetických incidentov, riadenie realizácie bezpečnostných opatrení, poradenskú a metodickú činnosť v oblasti informačnej a kybernetickej bezpečnosti a iné;

p) riešenie kybernetického bezpečnostného incidentu označuje všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzenie jeho následkov.

Článok III

PREDMET ZMLUVY

1. Podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti a s ohľadom na Hlavnú zmluvu je predmetom tejto Zmluvy určenie práv a povinností zmluvných strán pri zabezpečovaní plnenia bezpečnostných opatrení a oznamovacích povinností.

Článok IV

POVINNOSTI DODÁVATEĽA

1. Dodávateľ sa zaväzuje prijať a dodržiavať opatrenia kybernetickej bezpečnosti Prevádzkovateľa základných služieb v

2. The Contractor agrees with the security measures set out in this Contract.
3. The Contractor shall also comply with the security policies of the Operator of Essential Services, which have been demonstrably communicated to the Contractor in writing by the Operator of Essential Services. The Contractor declares to agree with the security policies of the Operator of Essential Services.
4. The Contractor agrees that the security policies of the Operator of Essential Services may be amended from time to time to reflect current security measures, the current state of the networks and information systems of the Operator of Essential Services, and current threats affecting the Contractor that could have a potential negative impact on the essential service provided by the Operator of Essential Services.
5. The Contractor undertakes to comply with their cybersecurity notification obligations to the extent set out in this Contract in order to meet the objectives hereof. A list of contacts of the Parties is specified in Annex 1 hereto.
6. The Contractor declares to have all the necessary technical, technological, and personnel equipment required to perform the tasks hereunder and to have in place the organisational, personnel and technical tasks, processes, roles and technologies necessary to meet the objectives hereof.
7. Remuneration for the performance of the Contractor's obligations hereunder and reimbursement of all costs incurred by the Contractor in connection with the performance of the Contractor's obligations hereunder shall be fully included in the monetary consideration provided by the Operator of Essential Services to the Contractor under the Main Agreement. No further monetary consideration shall be due to the Contractor from the Operator of Essential Services for the performance of the Contractor's obligations hereunder.
8. The Contractor agrees not to engage any other contractor (a **"subcontractor"**) to provide, in whole or in part, the performance of this Contract prior to receiving the written consent of the Operator of Essential Services. The list of subcontractors within the scope of provisions of Section 41 of Act No. 343/2015 Coll. on Public Procurement and on amendments to certain acts, as amended, shall form Annex 3 hereto. When selecting a subcontractor, the Contractor undertakes to check whether the subcontractor has

rozsahu uvedenom v tejto Zmluve tak, aby boli splnené ciele tejto Zmluvy. Zoznam bezpečnostných opatrení Prevádzkovateľa základných služieb a súvisiace nastavenie procesu riadenia kybernetickej bezpečnosti sú uvedené v prílohe č. 2 tejto Zmluvy.

2. Dodávateľ súhlasí s bezpečnostnými opatreniami uvedenými v tejto Zmluve.
3. Dodávateľ je tiež povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základných služieb, ktoré mu Prevádzkovateľ základných služieb preukázateľne písomne oznámil. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnou politikou Prevádzkovateľa základných služieb.
4. Dodávateľ súhlasí s tým, že bezpečnostné politiky Prevádzkovateľa základných služieb môžu byť priebežne menené a dopĺňané tak, aby odrážali aktuálne bezpečnostné opatrenia, aktuálny stav sietí a informačných systémov Prevádzkovateľa základných služieb a aktuálne hrozby, ktoré majú vplyv na Dodávateľa a ktoré by mohli mať potenciálny negatívny dopad na základné služby poskytované Prevádzkovateľom základných služieb.
5. Dodávateľ sa zaväzuje plniť svoje oznamovacie povinnosti v oblasti kybernetickej bezpečnosti v rozsahu stanovenom v tejto Zmluve tak, aby boli splnené ciele tejto Zmluvy. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto Zmluvy.
6. Dodávateľ vyhlasuje, že disponuje potrebným technickým, technologickým a personálnym vybavením potrebným na plnenie úloh podľa tejto Zmluvy a že má zavedené organizačné, personálne a technické úlohy, procesy, funkcie a technológie potrebné na plnenie cieľov tejto Zmluvy.
7. Odmena za plnenie záväzkov Dodávateľa podľa tejto Zmluvy a úhrada všetkých nákladov, ktoré Dodávateľovi vzniknú v súvislosti s plnením záväzkov Dodávateľa podľa tejto Zmluvy, je v plnej výške zahrnutá v peňažnom plnení, ktoré Prevádzkovateľ základných služieb poskytuje Dodávateľovi podľa Hlavnej zmluvy. Prevádzkovateľ základných služieb neposkytne Dodávateľovi žiadne ďalšie peňažné plnenie za plnenie záväzkov Dodávateľa podľa tejto Zmluvy.
8. Dodávateľ sa zaväzuje, že do úplného alebo čiastočného zabezpečenia plnenia tejto Zmluvy nezapojí žiadneho iného dodávateľa (ďalej len **„subdodávateľ"**) pred získaním písomného súhlasu Prevádzkovateľa

adequate technical and organisational support. The Contractor's obligations hereunder shall apply mutatis mutandis to the subcontractor. The Contractor shall be fully responsible to the Operator of Essential Services for the performance of the obligations of the subcontractor as if the Contractor was performing such obligations themselves.

Article V

SECURITY MEASURES

1. The Contractor undertakes to adopt and comply with minimum security measures in the fields under Section 20(3)(d), (f), (g), (k), (m) of the Cybersecurity Act to the extent of:

   under Sections 12, 10, 9, 15, 14 of Decree of the National Security Authority No. 362/2018 Coll., which establishes the content of security measures, the content and structure of security documentation and the scope of general security measures, and to the extent specified in the security policies of the Operator of Essential Services.
2. The Contractor undertakes to adopt and comply with sectoral security measures in the scope specified in the security policies of the Operator of Essential Services.
3. The Contractor declares to have established and implemented security measures under Section 20(3) of the Cybersecurity Act in the field of:
   a) access management,
   b) security of the operation of information systems and networks,
   c) vulnerability assessments and security updates,
   d) event logging and monitoring,
   e) handling cybersecurity incidents.
4. Security measures shall include as a minimum:
   - detection of cybersecurity incidents,
   - recording of cybersecurity incidents,
   - procedures for addressing and resolving cybersecurity incidents,
   - designation of a contact person to receive and record reports,
   - connection to the communication system for reporting and handling cybersecurity incidents and the central early warning system

základných služieb. Zoznam subdodávateľov v rozsahu ustanovení § 41 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov tvorí prílohu č. 3 tejto Zmluvy. Dodávateľ sa pri výbere subdodávateľa zaväzuje preveriť, či má subdodávateľ primerané technické a organizačné zabezpečenie. Povinnosti Dodávateľa vyplývajúce z tejto Zmluvy sa primerane vzťahujú aj na subdodávateľa. Dodávateľ v plnom rozsahu zodpovedá Prevádzkovateľovi základných služieb za plnenie povinností subdodávateľa, ako keby tieto povinnosti plnil sám.

Článok V

BEZPEČNOSTNÉ OPATRENIA

1. Dodávateľ sa zaväzuje prijať a dodržiavať minimálne bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. d), f), g), k), m) zákona o kybernetickej bezpečnosti v rozsahu:

   podľa § 12, 10, 9, 15, 14 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a v rozsahu uvedenom v bezpečnostných politikách Prevádzkovateľa základných služieb.
2. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu uvedenom v bezpečnostných politikách Prevádzkovateľa základných služieb.
3. Dodávateľ vyhlasuje, že má zavedené a implementované bezpečnostné opatrenia podľa § 20 ods. 3 zákona o kybernetickej bezpečnosti v oblasti:
   a) správy prístupu,
   b) bezpečnosti prevádzky informačných systémov a sietí,
   c) posudzovania zraniteľností a aktualizácie bezpečnostných údajov,
   d) zaznamenávania a monitorovania udalostí,
   e) riešenia kybernetických bezpečnostných incidentov.
4. Bezpečnostné opatrenia zahŕňajú minimálne:
   - odhaľovanie kybernetických bezpečnostných incidentov;

provided that this obligation applies to the Operator.

5. Security measures shall be adopted and implemented on the basis of approved security documentation, which shall be up-to-date and correspond to the actual situation in the organisation.
6. Content and structure of the safety documentation shall be as follows:
   - approved cybersecurity strategy and cybersecurity policies,
   - information classification and categorisation of networks and information systems,
   - documented definition of the scope and method of implementation of all security measures,
   - performed cybersecurity risk analysis.
7. During the term of this Contract, the Contractor agrees to have the technical, technological, and personnel equipment in place at the level necessary for the proper and timely performance hereof, and to have the organisational, personnel and technical tasks, processes, roles, and technologies in place at the level necessary to effectively meet the objectives hereof.
8. All Contractor's employees who will participate in the performance of the Main Agreement and the Contract and/or will have access to the information and data of the Operator of Essential Services shall be qualified under Contractor's Information Security Management Program. The Contractor shall bind the persons who will be involved in the performance under this clause to confidentiality under Section 12(1) of the Cybersecurity Act.
9. The Contractor agrees to establish procedures for the performance of the Contractor's obligations hereunder in security documentation, which shall be current and up-to-date; the Contractor shall provide the security documentation to the Operator of Essential Services for inspection and production of copies upon request.
10. The Contractor undertakes to adopt and comply with the general security measures in accordance with ISO 27001 and ISO 27701 (Information technology. Security methods. Code of practice for information security controls.) to the extent specified in the security policies of the Operator of Essential Services.

- zaznamenávanie kybernetických bezpečnostných incidentov;
- postupy na riešenie a vyriešenie kybernetických bezpečnostných incidentov;
- určenie kontaktnej osoby na prijímanie a zaznamenávanie hlásení;
- pripojenie na komunikačný systém na nahlasovanie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania za predpokladu, že sa táto povinnosť vzťahuje na Prevádzkovateľa.

5. Bezpečnostné opatrenia sa prijímajú a zavádzajú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a zodpovedať skutočnej situácii v organizácii.
6. Obsah a štruktúra bezpečnostnej dokumentácie musí byť nasledovná:
   - schválená stratégia kybernetickej bezpečnosti a politiky kybernetickej bezpečnosti,
   - klasifikácia informácií a kategorizácia sietí a informačných systémov,
   - zdokumentované vymedzenie rozsahu a spôsobu vykonávania všetkých bezpečnostných opatrení,
   - vykonaná analýza rizík kybernetickej bezpečnosti.
7. Dodávateľ sa zaväzuje, že počas trvania tejto Zmluvy bude mať zabezpečené technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto Zmluvy a organizačné, personálne a technické úlohy, procesy, funkcie a technológie na úrovni potrebnej na efektívne plnenie cieľov tejto Zmluvy.
8. Všetci zamestnanci Dodávateľa, ktorí sa budú podieľať na plnení Hlavnej zmluvy a Zmluvy a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základných služieb, musia mať kvalifikáciu podľa programu riadenia informačnej bezpečnosti Dodávateľa. Dodávateľ zaviaže osoby, ktoré sa budú podieľať na plnení podľa tohto bodu, k mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.
9. Dodávateľ sa zaväzuje stanoviť postupy pre plnenie povinností Dodávateľa podľa tejto Zmluvy v bezpečnostnej dokumentácii,

Article VI

PREVENTION OF CYBERSECURITY INCIDENTS

1. As part of the prevention of cybersecurity incidents that could have a potential negative impact on the essential service provided by the Operator of Essential Services or that could relate to the cybersecurity of the networks and information systems of the Operator of Essential Services ("**incidents**"), the Contractor undertakes to:
   a) ensure their own cybersecurity so that the networks and information systems of the Operator of Essential Services cannot be compromised through the Contractor;
   b) create and increase the security awareness of their employees who will participate in the performance of the Main Agreement and the Contract or will have access to information of the Operator of Essential Services;
   c) monitor alerts and warnings and other information to minimise, avert or remedy the consequences of incidents in general;
   d) monitor threats affecting the Contractor that could have a potential negative impact on the essential service provided by the Operator of Essential Services;
   e) prevent the occurrence of incidents;
   f) systematically collect (monitor and detect), centralise (record), analyse and evaluate information on incidents;
   g) receive incident warnings from the Operator of Essential Services and carry out preventive measures necessary to avert threats that could have a potential negative impact on the essential service provided by the Operator of Essential Services;
   h) send timely warnings to the Operator of Essential Services of incidents of which they become aware of from their own activities hereunder or otherwise; and
   i) cooperate with the Operator of Essential Services in providing cybersecurity of networks and information systems of the Operator of Essential Services.

Article VII

INCIDENT HANDLING PROCEDURE

1. The Contractor undertakes to report each incident within one (1) day to the Operator of Essential Services in the manner specified by the Operator of Essential Services, including

ktorá musí byť aktuálna; Dodávateľ je povinný poskytnúť bezpečnostnú dokumentáciu Prevádzkovateľovi základných služieb na nahliadnutie a na požiadanie vyhotoviť jej kópie.

10. Dodávateľ sa zaväzuje prijať a dodržiavať všeobecné bezpečnostné opatrenia v súlade s normami ISO 27001 a ISO 27701 (Informačné technológie. Bezpečnostné metódy. Kódex postupov pre kontrolu informačnej bezpečnosti.) v rozsahu uvedenom v bezpečnostných politikách Prevádzkovateľa základných služieb.

Článok VI

PREDCHÁDZANIE KYBERNETICKÝM BEZPEČNOSTNÝM INCIDENTOM

1. V rámci predchádzania kybernetickým bezpečnostným incidentom, ktoré by mohli mať potenciálny negatívny dopad na základné služby poskytované Prevádzkovateľom základných služieb alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základných služieb (ďalej len „**incidenty**"), sa Dodávateľ zaväzuje:
   a) zabezpečiť vlastnú kybernetickú bezpečnosť tak, aby prostredníctvom Dodávateľa nemohlo dôjsť k narušeniu sietí a informačných systémov Prevádzkovateľa základných služieb;
   b) vytvoriť a zvýšiť bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Hlavnej zmluvy a Zmluvy alebo budú mať prístup k informáciám Prevádzkovateľa základných služieb;
   c) monitorovať výstrahy a varovania a iné informácie s cieľom minimalizovať, odvrátiť alebo odstrániť následky incidentov vo všeobecnosti;
   d) monitorovať hrozby, ktoré majú vplyv na Dodávateľa a ktoré by mohli mať potenciálny negatívny vplyv na základné služby poskytované Prevádzkovateľom základných služieb;
   e) predchádzať vzniku incidentov;
   f) systematicky zhromažďovať (monitorovať a zisťovať), centralizovať (zaznamenávať), analyzovať a vyhodnocovať informácie o incidentoch;
   g) prijímať upozornenia na incidenty od Prevádzkovateľa základných služieb a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny negatívny vplyv na

the degree of severity identified on the basis of the exceeded criteria for each incident category. If the effects of the incident have not passed by the time the incident is reported, the Contractor undertakes to send an incomplete incident report indicating the identifier of the incomplete report and to complete the report as soon as the proper operation of the network and information system has been restored.

2. The Contractor undertakes to address incidents primarily by responding or otherwise reacting to the incident, restricting the incident and its impact, remediating the consequences of the incident, providing on-site incident response assistance, responding to the incident and support responses to the incident (the "**reactive measure**"). When resolving incidents, the Contractor shall, at the request of the Operator of Essential Services, cooperate with the Operator of Essential Services, the National Security Authority, and the Ministry of Economy of the Slovak Republic and, for this purpose, shall provide them with the necessary assistance and any information obtained from their own activities hereunder or otherwise that may be relevant to the resolution of the incident.
3. The Contractor undertakes to secure evidence or means of proof at the time of the incident so that it can be used in criminal proceedings and to provide it to the Operator of Essential Services.
4. The Contractor undertakes to inform the Operator of Essential Services of the fact that a criminal offence may have been committed in connection with the incident.
5. The Contractor undertakes to notify and demonstrate to the Operator of Essential Services without delay the implementation of the reactive measure and its outcome.
6. Upon resolution of the incident, the Contractor shall, at the request of the Operator of Essential Services, submit a proposal for measures to prevent further continuation, spread, and recurrence of the incident (hereinafter referred to as "**protective measures**") to the Operator of Essential Services for approval within a specified period of time. If the Contractor fails to propose a protective measure within the specified period of time, or if the proposed protective measure is manifestly ineffective, the Contractor shall cooperate with the Operator of Essential Services on their proposal.

základné služby poskytované Prevádzkovateľom základných služieb;

h) včas zasielať Prevádzkovateľovi základných služieb varovania o incidentoch, o ktorých sa dozvedeli z vlastnej činnosti podľa tejto Zmluvy alebo inak, a

i) spolupracovať s Prevádzkovateľom základných služieb pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základných služieb.

Článok VII
POSTUP PRI RIEŠENÍ INCIDENTOV

1. Dodávateľ sa zaväzuje nahlásiť každý incident do jedného (1) dňa Prevádzkovateľovi základných služieb spôsobom určeným Prevádzkovateľom základných služieb vrátane stupňa závažnosti určeného na základe prekročených kritérií pre jednotlivé kategórie incidentov. Ak následky incidentu do nahlásenia incidentu nepominú, Dodávateľ sa zaväzuje zaslať neúplné hlásenie o incidente s uvedením identifikátora neúplného hlásenia a hlásenie doplniť hneď po obnovení riadnej prevádzky siete a informačného systému.
2. Dodávateľ sa zaväzuje riešiť incidenty predovšetkým reagovaním na incident, obmedzením incidentu a jeho dopadov, odstránením následkov incidentu, poskytnutím pomoci pri riešení incidentu na mieste, reakciou na incident a podpornými reakciami na incident (ďalej len „**reaktívne opatrenie**"). Pri riešení incidentov je Dodávateľ povinný na požiadanie Prevádzkovateľa základných služieb spolupracovať s Prevádzkovateľom základných služieb, Národným bezpečnostným úradom a Ministerstvom hospodárstva Slovenskej republiky a za týmto účelom im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy alebo iným spôsobom, ktoré môžu byť relevantné pre riešenie incidentu.
3. Dodávateľ sa zaväzuje zabezpečiť dôkazy alebo dôkazné prostriedky v čase incidentu tak, aby mohli byť použité v trestnom konaní a poskytnúť ich Prevádzkovateľovi základných služieb.
4. Dodávateľ sa zaväzuje informovať Prevádzkovateľa základných služieb o skutočnosti, že v súvislosti s incidentom

7. Once the protective measure has been approved by the Operator of Essential Services, the Contractor shall implement the protective measure without undue delay. Once the protective measure has been implemented by the Contractor, the Contractor shall verify its effectiveness.

Article VIII
CONFIDENTIALITY OBLIGATION

1. The Contractor undertakes to maintain confidentiality regarding any facts of which the Contractor becomes aware in connection with the performance of the Main Agreement and the present Contract, and which are not publicly known, insofar as they may concern the field of cybersecurity. In case of doubt, the fact shall be deemed to concern the field of cybersecurity. In particular, the Contractor shall protect information which could affect the essential service provided by the Operator of Essential Services or which could relate to the cybersecurity of the networks and information systems of the Operator of Essential Services. The Contractor shall also protect all information provided by the Operator of Essential Services to the Contractor.
2. The confidentiality obligation under the present Article shall continue even after the termination of this Contract.
3. Exceptions to the confidentiality obligation under the present Article shall be governed by the Cybersecurity Act.
4. The Contractor undertakes to ensure that their employees, subcontractors and the subcontractors' employees observe the confidentiality obligation to the same extent, even after the termination of their employment, business relationship, or other relationship.
5. Upon termination of this Contract, the Contractor shall destroy all information to which the Contractor has had access during the term as directed by the Operator of Essential Services.

Article IX
CONTACT PERSONS IN THE FIELD OF CYBERSECURITY

1. During the performance of the Contractor's obligations of this Contract, the Contractor undertakes to communicate with the Operator of Essential Services in the manner specified by the Operator of Essential Services, and the Contractor shall have

mohol byť spáchaný trestný čin.

5. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Prevádzkovateľovi základných služieb vykonanie reaktívneho opatrenia a jeho výsledok.
6. Po vyriešení incidentu je Dodávateľ povinný na žiadosť Prevádzkovateľa základných služieb predložiť Prevádzkovateľovi základných služieb na schválenie v stanovenej lehote návrh opatrení na zamedzenie ďalšieho pokračovania, šírenia a opakovania incidentu (ďalej len „**ochranné opatrenia**"). Ak Dodávateľ nenavrhne ochranné opatrenie v stanovenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúčinné, Dodávateľ spolupracuje s Prevádzkovateľom základných služieb na jeho návrhu.
7. Po schválení ochranného opatrenia Prevádzkovateľom základných služieb je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po zavedení ochranného opatrenia Dodávateľom Dodávateľ overí jeho účinnosť.

Článok VIII
POVINNOSŤ ZACHOVÁVAŤ MLČANLIVOSŤ

1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením Hlavnej zmluvy a tejto Zmluvy a ktoré nie sú verejne známe, pokiaľ sa môžu týkať oblasti kybernetickej bezpečnosti. V prípade pochybností sa má za to, že sa daná skutočnosť týka oblasti kybernetickej bezpečnosti. Dodávateľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základné služby poskytované Prevádzkovateľom základných služieb alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základných služieb. Dodávateľ je tiež povinný chrániť všetky informácie, ktoré mu Prevádzkovateľ základných služieb poskytol.
2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení platnosti tejto Zmluvy.
3. Výnimky z povinnosti zachovávať mlčanlivosť podľa tohto článku sa riadia zákonom o kybernetickej bezpečnosti.
4. Dodávateľ sa zaväzuje zabezpečiť, aby jeho zamestnanci, subdodávatelia a zamestnanci subdodávateľov dodržiavali povinnosť zachovávať mlčanlivosť v rovnakom rozsahu aj po skončení ich pracovného, služobného či iného pomeru.

conditions in place to enable secure transmission of information.
2. The Operator of Essential Services shall designate contact persons for communication with the Contractor in the field of cybersecurity in Annex 1 hereto.
3. The Contractor shall designate contact persons for communication with the Operator of Essential Services for cybersecurity in Annex 1 hereto.
4. The contact persons set out in Annex 1 hereto may be changed by the relevant Party if such a Party notifies the other Party in writing of the new contact person; no amendment to this Contract shall be required for such change to take effect. The provisions of this Contract regarding notifications shall apply to the notification of new contact persons.

Article X

COMMON PROVISIONS

1. The Contractor agrees to perform its obligations in accordance with the Cybersecurity Act and its implementing regulations, including general security measures, security standards, cybersecurity knowledge standards and identification criteria for each category of cybersecurity incidents, operational procedures, methodologies, cyberspace behaviour policies, cybersecurity incident prevention policies and cybersecurity incident resolution policies issued by the National Security Authority in the field of cybersecurity.
2. The Contractor shall further comply with its obligations in accordance with the sectoral security measures issued by the Ministry of Health of the Slovak Republic in cooperation with the National Security Authority.
3. The Contractor undertakes to process information that could affect the essential service provided by the Operator of Essential Services or which could relate to the cybersecurity of the networks and information systems of the Operator of Essential Services in such a way that its availability, confidentiality, authenticity and integrity are not compromised.
4. The Contractor undertakes to have its documentation, information systems and other information and communication technologies relating to the performance of its obligations hereunder stored in a secure place in such a way that their confidentiality, authenticity, and integrity are not compromised.
5. The Contractor undertakes to document its

5. Po skončení platnosti tejto Zmluvy je Dodávateľ povinný zničiť všetky informácie, ku ktorým mal počas platnosti Zmluvy prístup, podľa pokynov Prevádzkovateľa základných služieb.

Článok IX

KONTAKTNÉ OSOBY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

1. Počas plnenia záväzkov Dodávateľa vyplývajúcich z tejto Zmluvy sa Dodávateľ zaväzuje komunikovať s Prevádzkovateľom základných služieb spôsobom určeným Prevádzkovateľom základných služieb, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce bezpečný prenos informácií.
2. Prevádzkovateľ základných služieb určí kontaktné osoby pre komunikáciu s Dodávateľom v oblasti kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy.
3. Dodávateľ určí kontaktné osoby pre komunikáciu s Prevádzkovateľom základných služieb v oblasti kybernetickej bezpečnosti v prílohe č. 1 tejto Zmluvy.
4. Kontaktné osoby uvedené v prílohe č. 1 tejto Zmluvy môže príslušná zmluvná strana zmeniť, ak písomne oznámi druhej zmluvnej strane novú kontaktnú osobu; na nadobudnutie účinnosti takejto zmeny sa nevyžaduje dodatok k tejto Zmluve. Na oznámenie nových kontaktných osôb sa vzťahujú ustanovenia tejto Zmluvy týkajúce sa oznámení.

Článok X

SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje plniť si povinnosti v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi vrátane všeobecných bezpečnostných opatrení, bezpečnostných noriem, noriem znalostí o kybernetickej bezpečnosti a kritérií identifikácie jednotlivých kategórií kybernetických bezpečnostných incidentov, prevádzkových postupov, metodík, zásad správania sa v kybernetickom priestore, zásad prevencie kybernetických bezpečnostných incidentov a zásad riešenia kybernetických bezpečnostných incidentov vydaných Národným bezpečnostným úradom v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je ďalej povinný plniť si povinnosti v súlade s odvetvovými bezpečnostnými opatreniami vydanými Ministerstvom zdravotníctva Slovenskej republiky v spolupráci s Národným bezpečnostným

activities (including recording incidents and documenting the training of their employees). 6. The Contractor undertakes to perform its obligations without delay unless otherwise specified in this Contract or in the requirements of applicable Slovak and EU legislation. 7. If the Contractor performs the Contract through a subcontractor who is wholly or partly providing performance for the Operator of Essential Services, or such performance is directly related to the operation of the networks and information systems of the Operator of Essential Services, the Contractor undertakes to ensure that their subcontractors also perform their cybersecurity obligations hereunder in order to meet the objectives hereof. The Contractor undertakes to ensure that the Operator of Essential Services can also audit these subcontractors in accordance with the provisions hereof. 8. In the event that the Contractor causes any damage to the Operator of Essential Services by violating their obligations under the relevant legislation and/or the Contract, the liability for damage and the obligation to compensate for the damage caused shall be governed by and in accordance with the provisions of Sections 373 et seq. of Act No. 513/1991 Coll., the Commercial Code, as amended. For the avoidance of doubt, the liability of the Contractor shall not be excluded by an obstacle that arose only at the time when the Contractor was in default of their obligation or by an obstacle arising from their economic conditions, but shall be excluded if the obstacle was force majeure. The damage also refers to the damage caused to the Operator of Essential Services due to having to incur costs as a result of the Contractor's breach of obligations. 9. The address for the delivery of documents refers to the individual addresses of the Parties, and the procedure for notifications, is set out in the Contract. Each Party shall inform the other Party in writing of any change to the delivery of documents no later than 5 working days after such change occurs. If, by reason of delay or failure to give notice of a change of the delivery address, a document cannot be delivered in a timely and proper manner to the other Party, the date of the unsuccessful attempt to redeliver the document shall be deemed to be the date of delivery of the document to the other Party, with all the legal consequences for the Party concerned. 10. The Contractor undertakes to notify all facts	úradom. **3.** Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základné služby poskytované Prevádzkovateľom základných služieb alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základných služieb tak, aby nebola ohrozená ich dostupnosť, dôvernosť, autentickosť a integrita. 4. Dodávateľ sa zaväzuje mať svoju dokumentáciu, informačné systémy a iné informačné a komunikačné technológie súvisiace s plnením svojich povinností podľa tejto Zmluvy uložené na bezpečnom mieste tak, aby nebola ohrozená ich dôvernosť, autentickosť a integrita. 5. Dodávateľ sa zaväzuje dokumentovať svoju činnosť (vrátane zaznamenávania incidentov a dokumentovania školení svojich zamestnancov). 6. Dodávateľ sa zaväzuje plniť si povinnosti bezodkladne, ak nie je v tejto Zmluve alebo v požiadavkách platných právnych predpisov Slovenskej republiky a EÚ uvedené inak. 7. Ak Dodávateľ plní Zmluvu prostredníctvom subdodávateľa, ktorý úplne alebo čiastočne zabezpečuje plnenie pre Prevádzkovateľa základných služieb, alebo takéto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základných služieb, Dodávateľ sa zaväzuje zabezpečiť, aby si aj jeho subdodávatelia plnili svoje povinnosti v oblasti kybernetickej bezpečnosti podľa tejto Zmluvy tak, aby boli naplnené ciele tejto Zmluvy. Dodávateľ sa zaväzuje zabezpečiť, aby aj Prevádzkovateľ základných služieb mohol u týchto subdodávateľov vykonať audit v súlade s ustanoveniami tejto Zmluvy. 8. V prípade, že Dodávateľ spôsobí Prevádzkovateľovi základných služieb akúkoľvek škodu porušením svojich povinností vyplývajúcich z príslušných právnych predpisov a/alebo Zmluvy, zodpovednosť za škodu a povinnosť nahradiť spôsobenú škodu sa riadi a bude riadiť ustanoveniami § 373 a nasl. zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov. Aby sa predišlo pochybnostiam, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti, ani prekážka vyplývajúca z jeho ekonomickej situácie, ale vylučuje ju prekážka vyššej moci. Škoda označuje aj škodu spôsobenú Prevádzkovateľovi základných služieb tým, že musel vynaložiť náklady v dôsledku porušenia povinností

affecting the Contract, as well as to report any other information requested by the Operator of Essential Services, in writing to the registered office address of the Operator of Essential Services.

Article XI

CYBERSECURITY AUDIT

1. No more than once each year, unless the Operator has a reasonably held belief that Contractor is in breach of its obligations under this this Contract, the Operator of Essential Services shall be entitled to conduct an audit of the Contractor to verify the fulfilment of the Contractor's obligations hereunder and the effectiveness of their fulfilment, in particular, to verify the technical, technological and personnel equipment of the Contractor for the fulfilment of tasks in the field of cybersecurity, as well as the setup of processes, roles and technologies in the organisational, personnel and technical fields of the Contractor for the fulfilment of the objectives hereof. For clarity, Contractor can meet its obligations under this Article XI by providing Operator with a copy of Contractor's ISO 27001 and ISO 27701 then-current certifications.
2. The Contractor shall submit a final report on the results of the audit conducted by the Operator to the National Security Authority (NSA) together with corrective measures and deadlines for removal of deficiencies within 30 days from the completion of the audit.
3. Any deficiencies identified in the audit by the Operator of Essential Services shall be corrected by the Contractor without undue delay, but no later than 60 calendar days or within a time period agreed to in writing by the Contractor in the audit report drawn up by the Operator.
4. The Operator of Essential Services may audit the Contractor either themselves or through a third party, in which case the rights and obligations of the Operator of Essential Services in carrying out the audit shall be exercised by a third party authorised by the Operator of Essential Services.
5. The Contractor undertakes to cooperate with the Operator of Essential Services in the audit and make available, documentation and technical and technological equipment related to the performance of tasks in the field of cybersecurity hereunder or to provide other necessary assistance.
6. In the course of the audit, the Operator of Essential Services shall be entitled to ask questions of the Contractor's employees

Dodávateľa.

9. Adresa na doručovanie písomností označuje jednotlivé adresy zmluvných strán a postup pri nahlasovaní je uvedený v Zmluve. Každá zmluvná strana je povinná písomne informovať druhú zmluvnú stranu o akejkoľvek zmene v doručovaní písomností najneskôr do 5 pracovných dní od vzniku takejto zmeny. Ak z dôvodu omeškania alebo neoznámenia zmeny adresy na doručovanie nie je možné písomnosť riadne a včas doručiť druhej zmluvnej strane, dátum neúspešného pokusu o opätovné doručenie písomnosti sa považuje za dátum doručenia písomnosti druhej zmluvnej strane so všetkými právnymi dôsledkami pre dotknutú zmluvnú stranu.
10. Dodávateľ sa zaväzuje oznámiť všetky skutočnosti, ktoré majú vplyv na Zmluvu, ako aj oznámiť akékoľvek iné informácie požadované Prevádzkovateľom základných služieb, a to písomne na adresu sídla Prevádzkovateľa základných služieb.

Článok XI

AUDIT KYBERNETICKEJ BEZPEČNOSTI

1. Prevádzkovateľ základných služieb je oprávnený vykonať u Dodávateľa audit, ktorého cieľom je overiť plnenie povinností Dodávateľa podľa tejto Zmluvy a účinnosť ich plnenia, a to najviac raz ročne, pokiaľ Prevádzkovateľ nemá dôvodné podozrenie, že Dodávateľ porušuje svoje povinnosti vyplývajúce z tejto Zmluvy, najmä overiť technické, technologické a personálne vybavenie Dodávateľa na plnenie úloh v oblasti kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti Dodávateľa na plnenie cieľov tejto Zmluvy. Pre prehľadnosť možno uviesť, že Dodávateľ môže splniť svoje povinnosti podľa tohto článku XI tým, že poskytne Prevádzkovateľovi kópiu vtedy platných certifikátov Dodávateľa ISO 27001 a ISO 27701.
2. Dodávateľ predloží Národnému bezpečnostnému úradu (NBÚ) záverečnú správu o výsledkoch auditu vykonaného Prevádzkovateľom spolu s nápravnými opatreniami a termínmi odstránenia nedostatkov do 30 dní od ukončenia auditu.
3. Všetky nedostatky zistené pri audite Prevádzkovateľa základných služieb je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však do 60 kalendárnych dní alebo v lehote písomne odsúhlasenej Dodávateľom v správe z auditu vypracovanej

involved in the performance of cybersecurity tasks hereunder.

7. As part of the audit, the Contractor shall demonstrate to the Operator of Essential Services compliance with the present Contract, in particular their readiness to perform the cybersecurity tasks hereunder, the up-to-date and high security awareness of their employees, the instructions given to their employees, subcontractors and the subcontractors' employees regarding the confidentiality obligations hereunder and their commitment to maintain such confidentiality, and the up-to-date status of their security documentation.
8. The Operator of Essential Services agrees to inform the Contractor at least thirty (30) working days in advance of their intention to conduct an audit at the Contractor. The performance or non-performance of the audit by the Operator of Essential Services shall not relieve the Contractor of their responsibility for the performance of the Contractor's obligations hereunder. If the Contractor fails to allow an audit to be carried out, the Contractor shall be deemed to have failed to perform their cybersecurity duties hereunder.
9. The Contractor undertakes to inform the Operator of Essential Services in writing of any change that has a significant impact on the security measures implemented by the Contractor.
10. The Operator of Essential Services undertakes to keep confidential any circumstances of which they become aware in the course of the audit and which are not public knowledge. The provisions of Article VIII (2), (3), and (4) hereof shall apply mutatis mutandis.

Article XII

FINAL PROVISIONS

1. The term of this Contract shall be concurrent with the term of the Main Agreement.
2. The Operator of Essential Services shall be entitled to terminate this Contract:
   a) if the Contractor commits a material breach of this Contract;
   b) if the Contractor is declared bankrupt or has been granted restructuring, or if the declaration of bankruptcy has been rejected or annulled due to lack of assets;
   c) if the Contractor is in liquidation.
3. The following shall constitute a material breach of this Contract:
   a) breach of obligations set out in Article IV(1), (8), Article VI(3), (4), Article VII and

Prevádzkovateľom.

4. Prevádzkovateľ základných služieb môže vykonať audit u Dodávateľa sám alebo prostredníctvom tretej osoby, pričom v takom prípade práva a povinnosti Prevádzkovateľa základných služieb pri výkone auditu vykonáva tretia osoba poverená Prevádzkovateľom základných služieb.
5. Dodávateľ sa zaväzuje spolupracovať s Prevádzkovateľom základných služieb pri audite a sprístupniť dokumentáciu a technické a technologické vybavenie súvisiace s plnením úloh v oblasti kybernetickej bezpečnosti podľa tejto Zmluvy, prípadne poskytnúť inú potrebnú súčinnosť.
6. Počas auditu je Prevádzkovateľ základných služieb oprávnený klásť otázky zamestnancom Dodávateľa, ktorí sa podieľajú na plnení úloh v oblasti kybernetickej bezpečnosti podľa tejto Zmluvy.
7. V rámci auditu Dodávateľ preukáže Prevádzkovateľovi základných služieb súlad s touto Zmluvou, najmä svoju pripravenosť na plnenie úloh kybernetickej bezpečnosti podľa tejto Zmluvy, aktuálnu a vysokú bezpečnostnú informovanosť svojich zamestnancov, poučenie svojich zamestnancov, subdodávateľov a zamestnancov subdodávateľov o povinnostiach zachovávať mlčanlivosť podľa tejto Zmluvy a ich záväzok zachovávať túto mlčanlivosť a aktuálny stav svojej bezpečnostnej dokumentácie.
8. Prevádzkovateľ základných služieb sa zaväzuje informovať Dodávateľa najmenej tridsať (30) pracovných dní vopred o svojom zámere vykonať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu zo strany Prevádzkovateľa základných služieb nezbavuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa podľa tejto Zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že Dodávateľ nesplnil svoje povinnosti v oblasti kybernetickej bezpečnosti podľa tejto Zmluvy.
9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základných služieb o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia zavedené Dodávateľom.
10. Prevádzkovateľ základných služieb sa zaväzuje zachovávať mlčanlivosť o všetkých okolnostiach, o ktorých sa dozvie v priebehu auditu a ktoré nie sú verejne známe. Ustanovenia článku VIII ods. 2, 3 a 4 tejto Zmluvy sa uplatňujú primerane.

Article VIII of this Contract;
b) if the Contractor fails to provide the necessary co-operation under this Contract.

4. The present Contract may be terminated by the Operator of Essential Services by a written notice of termination, even without providing a reason, with a notice period of 1 month commencing on the first day of the month following the month in which the notice of termination is delivered to the Contractor. For clarity, the Operator of Essential Services' termination of this Contract for convenience shall not be deemed to be a termination of the Main Agreement.
5. The Parties agree that the present Contract may also be terminated by a written agreement of the Parties.
6. The termination hereof shall not affect those provisions which, by their nature or their express wording, are intended to survive the termination hereof and the obligations for damages resulting from the breach of obligations hereunder.
7. The present Contract shall be governed by the laws of the Slovak Republic without regard to conflict-of-law rules. The legal relationships not expressly regulated hereby shall be governed by the relevant provisions of the Commercial Code and other related generally binding legislation.
8. Any disputes arising herefrom shall be settled primarily out of court. By signing the present Agreement, the Parties confirm that the courts of the Slovak Republic are competent to settle any disputes arising herefrom.
9. This Contract may be changed, amended, or terminated solely by a written agreement of the Parties.
10. Neither Party shall be entitled to assign their rights and obligations under this Contract to another person without the prior written consent of the other Party, except that a Party may, on written notice to the other Party, assign it rights to a purchaser of all, or substantially all, of its assets.
11. If any provision is deemed by a court, or other competent authority to be invalid or unenforceable, such provision shall be void only to the relevant and the narrowest extent possible, and the remaining provisions shall remain in full force and effect. In such an event, the Parties shall ensure that the purpose of the provisions that are deemed to be unenforceable or void shall be respected to the maximum extent possible and shall be legally binding to the Parties in a legally

Článok XII
ZÁVEREČNÉ OPATRENIA

1. Doba platnosti tejto Zmluvy sa zhoduje s dobou platnosti Hlavnej zmluvy.
2. Prevádzkovateľ základných služieb je oprávnený túto Zmluvu vypovedať:
   a) ak sa Dodávateľ dopustí podstatného porušenia tejto Zmluvy;
   b) ak je na Dodávateľa vyhlásený konkurz alebo povolená reštrukturalizácia, alebo ak bolo vyhlásenie konkurzu zamietnuté alebo zrušené pre nedostatok majetku;
   c) ak je Dodávateľ v likvidácii.
3. Za podstatné porušenie tejto Zmluvy sa považuje:
   a) porušenie povinností uvedených v článku IV ods. 1 a 8, článku VI ods. 3 a 4, článku VII a článku VIII tejto Zmluvy;
   b) situácia, kedy Dodávateľ neposkytne potrebnú súčinnosť podľa tejto Zmluvy.
4. Túto Zmluvu môže Prevádzkovateľ základných služieb vypovedať písomnou výpoveďou, a to aj bez uvedenia dôvodu, pričom výpovedná lehota je 1 mesiac a začína plynúť prvým dňom mesiaca nasledujúcim po mesiaci, v ktorom bola výpoveď doručená Dodávateľovi. Kvôli jednoznačnosti sa výpoveď tejto Zmluvy zo strany Prevádzkovateľa základných služieb z dôvodu výhodnosti nepovažuje za výpoveď Hlavnej zmluvy.
5. Zmluvné strany sa dohodli, že táto Zmluva môže byť ukončená aj písomnou dohodou zmluvných strán.
6. Ukončenie tejto Zmluvy nemá vplyv na tie ustanovenia, ktoré vzhľadom na svoju povahu alebo výslovné znenie majú trvať aj po ukončení tejto Zmluvy, a záväzky na náhradu škody vyplývajúce z porušenia povinností podľa tejto Zmluvy.
7. Táto Zmluva sa riadi právnym poriadkom Slovenskej republiky bez ohľadu na kolízne normy. Právne vzťahy výslovne neupravené touto Zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.
8. Prípadné spory, ktoré z tejto Zmluvy vyplynú, sa budú riešiť predovšetkým mimosúdne. Zmluvné strany podpisom tejto Zmluvy potvrdzujú, že právomoc na riešenie sporov vyplývajúcich zo Zmluvy majú súdy Slovenskej republiky.
9. Túto Zmluvu je možné meniť, dopĺňať alebo ukončiť výlučne písomnou dohodou zmluvných strán.
10. Žiadna zo zmluvných strán nie je oprávnená

enforceable form.

12. This Contract constitutes the entire agreement of the Parties relating to the subject matter in question, and terminates all previous written and oral contracts regarding the subject matter and neither Party may rely on any special oral or written arrangements or agreements not specified in this Contract.
13. This Contract is drawn up in two (2) counterparts, one for each Party.
14. The Parties acknowledge that the Operator of Essential Services is an obliged person under Section 2(1) of Act No. 211/2000 Coll. on free access to information and on amendment and supplements to certain acts (Freedom of Information Act), as amended, and therefore the present Contract is a compulsory contract under Section 5(a) of this Act in conjunction with Section 47(a) of Act No. 40/1964 Coll. of the Civil Code, as amended.
15. The following annexes form an integral part of this Contract:
    - Annex 1 – List of job roles and contacts of the Operator of Essential Services and the Contractor
    - Annex 2 – Security measures in the organisation of the Operator of Essential Services applicable to the Contractor – Directive of the Operator of Essential Services, Third-party requirements and security measures FN TT No. SM-2021-16
    - Annex 3 – List of subcontractors
16. The Parties declare that they have full capacity to perform legal acts, that their legal capacity is not limited, that this Contract has not been concluded in distress or under conspicuously unfavourable conditions, that they have carefully read the contents of this Contract and as a sign of it being clear, comprehensible and expressing their free, earnest, and common will, sign this Contract.

postúpiť svoje práva a povinnosti vyplývajúce z tejto Zmluvy na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany, s tým, že zmluvná strana môže na základe písomného oznámenia druhej zmluvnej strane postúpiť svoje práva na nadobúdateľa celého majetku alebo jeho podstatnej časti.

11. Ak súd alebo iný príslušný orgán považuje niektoré ustanovenie za neplatné alebo nevymáhateľné, toto ustanovenie je neplatné len v príslušnom a najužšom možnom rozsahu a ostatné ustanovenia zostávajú v plnej platnosti a účinnosti. V takomto prípade zmluvné strany zabezpečia, aby sa účel ustanovení, ktoré sa považujú za nevymáhateľné alebo neplatné, dodržal v maximálnej možnej miere a aby boli pre zmluvné strany právne záväzné v právne vynútiteľnej forme.
12. Táto Zmluva predstavuje úplnú dohodu zmluvných strán týkajúcu sa predmetu Zmluvy a ruší všetky predchádzajúce písomné a ústne zmluvy týkajúce sa predmetu Zmluvy a žiadna zo zmluvných strán sa nemôže odvolávať na žiadne osobitné ústne alebo písomné dojednania alebo dohody, ktoré nie sú uvedené v tejto Zmluve.
13. Táto Zmluva je vyhotovená v dvoch (2) rovnopisoch, z ktorých každá Zmluvná strana obdrží jeden.
14. Zmluvné strany berú na vedomie, že Prevádzkovateľ základných služieb je povinnou osobou podľa § 2 ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov, a preto je táto Zmluva povinne zverejňovanou zmluvou podľa § 5 písm. a) tohto zákona v spojení s § 47 písm. a) zákona č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov.
15. Nasledujúce prílohy tvoria neoddeliteľnú súčasť tejto Zmluvy:
    - Príloha č. 1 – Zoznam pracovných pozícií a kontaktov Prevádzkovateľa základných služieb a Dodávateľa
    - Príloha č. 2 – Bezpečnostné opatrenia v organizácii Prevádzkovateľa základných služieb platné pre Dodávateľa – smernica Prevádzkovateľa základných služieb, požiadavky tretích strán a bezpečnostné opatrenia FN TT č. SM-2021-16
    - Príloha č. 3 – Zoznam subdodávateľov
16. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich

	spôsobilosť na právne úkony nie je obmedzená, že táto Zmluva nebola uzatvorená v tiesni ani za nápadne nevýhodných podmienok, že si pozorne prečítali obsah tejto Zmluvy a na znak toho, že je Zmluva jasná, zrozumiteľná a vyjadruje ich slobodnú, vážnu a spoločnú vôľu, ju podpisujú.

	iSchemaView, Inc.	**University Hospital Trnava / Fakultná nemocnica Trnava**
Signature / Podpis		
Name / Meno	Jim Rosa	JUDr. Vladislav Šrojta
Title / Pozícia	SVP Regulatory & Quality / Senior viceprezident pre reguláciu a kvalitu	CEO / Riaditeľ
Date / Dátum		

Annex 1 **Contractor's Job Roles & Technical Support Employees**	**Príloha 1** **Pracovné úlohy a zamestnanci technickej podpory Dodávateľa**
Operator's Designate Contact/s TO BE PROVIDED BY CUSTOMER	**Kontaktné osoby určené Prevádzkovateľom** POSKYTNE ZÁKAZNÍK
Contractor's Designate Contact/s Technical Team Tel: +1.650.388.9767 Ext 2. E-Mail: support@ischemaview.com	**Kontaktné osoby určené Dodávateľom** Technický tím Tel. č.: +1.650.388.9767 klapka 2. E-mail: support@ischemaview.com
Contractor's Job Role Provision of remote technical support, including installation, optimization, maintenance and support of Contractor's proprietary software installed on Operator of Essential Services server.	**Pracovné úlohy Dodávateľa** Poskytovanie vzdialenej technickej podpory vrátane inštalácie, optimalizácie, údržby a podpory vlastného softvéru Dodávateľa nainštalovaného na serveri Prevádzkovateľa základných služieb.
Contractor's Technical Support Employees Employees located in the EU who are qualified under Contractor's Information Management Program that comprises physical, technical and administrative safeguards that are no lower than accepted industry practice, and that include: (1) authentication and access control; (2) the training of personnel on the Program; (3) monitoring and regular testing of the Program; and (4) prompt modification of the Program to remedy any weaknesses detected as a result of (3), and to address known and potential security threats.	**Zamestnanci technickej podpory Dodávateľa** Zamestnanci so sídlom v EÚ kvalifikovaní v rámci programu riadenia informácií Dodávateľa, ktorý zahŕňa fyzické, technické a administratívne bezpečnostné opatrenia, ktoré nie sú nižšie ako osvedčené odvetvové postupy a ktoré zahŕňajú: (1) autentifikáciu a kontrolu prístupu, (2) školenie personálu o programe, (3) monitorovanie a pravidelné testovanie programu a (4) okamžitú úpravu programu s cieľom napraviť všetky nedostatky zistené v dôsledku opatrení uvedených v bode (3) a riešiť existujúce a potenciálne bezpečnostné hrozby.
Appendix 2 – Security measures in the organization of the Operator of basic services relating to the Supplier – Directive of the Operator of basic services, requirements of third parties and security measures FN TT no. SM-2021-16	**Príloha 2 – Bezpečnostné opatrenia v organizácii Prevádzkovateľa základných služieb vzťahujúce sa na Dodávateľa – Smernica Prevádzkovateľa základných služieb, požiadavky tretích strán a bezpečnostné opatrenia FN TT č. SM-2021-16**
Annex 3 **List of Approved Sub-contractors**	**Príloha 3** **Zoznam schválených subdodávateľov**
AWS EU	AWS EU