Vendor Cybersecurity Requirements

1. Information Security Management System

1.1. In providing services, the Supplier undertakes to apply security policies and processes ensuring the protection of data and information created and processed during the provision of services. Based on security needs and the results of risk assessments, the Supplier is required to implement appropriate security measures, continuously monitor them, and evaluate their effectiveness.

1.2. The Supplier further undertakes to maintain records of the creation and processing of data and information within the scope of the services provided, to document all material circumstances related to their security, and to make these records available to the Customer upon request.

1.3. At the same time, the Supplier is obligated to establish and maintain up-to-date security measures in the form of processes and technologies that ensure compliance with the security policy.

2. Risk Management

2.1. In providing the services, the Supplier undertakes to manage its own risks that may affect the provision of such services.

3. Organizational Security Requirements

3.1. In connection with the provision of services, the Supplier undertakes, in particular, to fulfill the following obligations:

a) no later than 5 days from the conclusion of the Agreement, appoint a responsible contact person for the purpose of ensuring compliance with these cybersecurity requirements and related communication between the contracting parties (hereinafter the “Contact Person”) and, within the same period, notify the Client in writing of the Contact Person’s details. The designation of a Contact Person for cybersecurity on the Supplier’s side does not affect the provisions of the Contract regarding authorized persons;

b) ensure that services are provided exclusively by authorized persons who have been duly familiarized with the relevant provisions of the Customer’s internal regulations and who possess the verified qualifications, knowledge, and experience necessary for the proper provision of services.

4. Management of Subcontractors

4.1. The Supplier further undertakes:

a) ensure compliance with cybersecurity requirements in contractual relationships with its subcontractors, if they are involved in the provision of services. At the same time, the Supplier is obligated to provide the Client with a written declaration of their compliance with cybersecurity requirements within 10 days of the effective date of the Agreement in which the subcontractors are involved;

b) enter into separate agreements with its subcontractors, employees, and other persons involved in the performance of this Agreement, if personal data is processed in the course of providing services, in accordance with the relevant provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

5. Human Resources Security

5.1. To the extent of the provision of services, the Supplier undertakes, upon request, to demonstrate to the Customer that all persons involved in the provision of services have been demonstrably familiarized with these cybersecurity requirements and with the relevant provisions of the Customer’s internal management regulations, whereby demonstrable familiarization is considered to include, in particular, training of the Provider’s employees arranged by the Client, the handover of relevant documentation in written or electronic form, or access arranged by the Client to a shared repository containing the relevant internal regulations.

5.2. The Provider is obligated to comply with the relevant provisions of the Client’s internal management regulations to the extent that it has been made aware of such regulations, and, if the services provided include a monitoring service, to define and fulfill the roles and responsibilities for monitoring the network and equipment within the scope of the services provided.

5.3. The Provider undertakes to ensure that persons involved in providing services to the Client in the Client’s environment or using the Client’s resources:

a) use only approved means for storing and sharing data and information on ;

b) do not store or share data and information of ethically inappropriate content that is contrary to good morals or damaging to the Client’s reputation;

c) not download, share, save, archive, or install data or executable files in violation of the license terms or copyright laws;

d) not visit websites with ethically inappropriate content;

e) not attempt to gain unauthorized access to the Customer’s resources or to the resources of other entities;

f) not attempt to make unauthorized modifications or other unauthorized interventions in the Client’s resources, even if the Client’s resources have been entrusted to their management;

g) not participate, through the Client’s resources, in the distribution of spam or malicious software.

5.4. The foregoing also applies to the use of resources outside the Client’s environment.

5.5. The Supplier acknowledges that a condition for granting access to the Client’s resources is the processing of personal data of the Supplier’s employees who are involved in the performance of the subject matter of the Agreement. If the Client is not permitted to process such personal data, access to the resources will not be granted.

6. Operations and Communications Management

6.1. The Supplier undertakes to ensure the secure operation of the information system and infrastructure used to provide services and further to ensure that only applications and technologies compliant with applicable Czech and European legislation are used for these purposes, particularly with regard to licensing terms and copyright law.

6.2. Upon request, the Supplier shall provide the Customer with an overview or report on the security measures implemented in its information system and infrastructure.

7. Change Management

7.1. The Supplier undertakes to respond appropriately to changes requested by the Customer and to adjust its technical and organizational measures accordingly so that they correspond to the new state following the implementation of the change.

7.2. The Supplier further undertakes to actively cooperate with the Customer in testing every significant change.

8. Access and Authorization Management

8.1. The Supplier undertakes to grant permissions to its employees only to the extent necessary for the performance of their duties, in such a way as to minimize the risks of unauthorized access to the Client’s resources. Granted access may not be shared by multiple persons, unless required by the technology used; in such a case, the Supplier is obligated to maintain records of the use of shared access and to submit these records to the Client upon request.

8.2. The Supplier shall further ensure that all persons involved in the provision of services protect authentication credentials and data and do not provide unauthorized access to other persons. At the same time, the Supplier is obligated to continuously monitor and evaluate the legitimacy and necessity of access for all persons who have access to the Client’s environment.

9. Access Authorization and Management Policies

9.1. The Supplier acknowledges that access to the ICT system may only be granted to its employees or the employees of its subcontractors, based on its request.

9.2. The assignment of permissions to employees is governed by the principle of the necessary minimum and is not an entitlement. In the event of unsuccessful user authentication attempts, the relevant account may be blocked and considered a security incident. In such a case, security incident management procedures may be applied, including the immediate revocation of access to the Client’s information assets.

10. Implementation and Documentation

10.1. The Supplier undertakes to ensure the secure implementation, innovation, updating, and testing of the technologies that are the subject of the performance, and further to provide the Customer with documentation containing, in particular:

a) all security settings, functions, and mechanisms;

b) a description of the authentication and authorization concept for assigning permissions;

c) installation and configuration procedures.

11. Software Development

11.1. If the subject matter of the service includes software development, the Supplier undertakes to:

a) comply with and implement the best practices for secure software development as specified in the contractual relationship;

b) upon request, allow an audit of completed or ongoing work and, upon its completion, submit the developed code and code review outputs, in particular to verify whether the work is being or was performed in accordance with the Contract and these cybersecurity requirements;

c) provide reasonable cooperation during security testing both during development and after the software has been delivered;

d) ensure that the performance includes only objectively necessary and contractually agreed components;

e) use current versions of products compatible with the Customer's environment when installing operating systems or third-party software;

f) ensure the security of the testing environment and the protection of test data;

g) deliver to the production environment only the contractually specified compiled or executable code and the data necessary for its operation;

h) guarantee that the supplied software will comply with the Customer's security policies and standards, with which it has been demonstrably familiarized, and that such compliance will be tested;

i) install the software exclusively in accordance with pre-approved migration procedures;

j) not to develop, compile, or distribute in the Customer's environment any program code intended for illegal control, disruption of availability, confidentiality, or integrity, or unauthorized or illegal acquisition of data and information.

12. Cybersecurity Events and Incidents

12.1. The Supplier undertakes to define and describe the activities, roles, and responsibilities necessary for the rapid and effective management of security incidents. Furthermore, the Supplier is obligated to immediately report to the Customer all security events and incidents with a potentially negative impact, via the designated communication channel or the Contact Person. At the same time, the Supplier is obligated to evaluate and retain information about incidents in accordance with applicable Czech and European legislation and to actively cooperate with the Customer, including by providing relevant information about suspicious devices or individuals.

12.2. Upon agreement with the Client, the Supplier is obligated to take reasonable measures to mitigate the impact of the incident or to resolve it. The Supplier is also obligated to cooperate in analyzing the causes of the incident and to propose measures to prevent its recurrence if the Supplier caused or contributed to the incident

13. Contractor's Liability

13.1. The Supplier acknowledges that a security incident or other breach of cybersecurity requirements caused by a factor on its part shall not be considered a circumstance excluding its liability for delay in the proper and timely performance of the subject matter of the Contract and shall not give rise to a right to compensation for any damage to the Supplier or a third party on the part of the Client. This provision shall not prejudice other provisions of the Contract regarding the Supplier's liability for delay.

14. Service Continuity

14.1. The Supplier undertakes to maintain adequate continuity of its assets necessary for the provision of services. At the same time, the Supplier undertakes to regularly verify and test its ability to ensure such continuity in accordance with the agreed service level.

15. Inspection and Audit

15.1. The Supplier undertakes, in connection with the provision of services, to provide reasonable cooperation during inspections conducted by the Customer or the relevant authorities.

16. Physical Security

16.1. The Supplier undertakes to comply with the operating rules of buildings and premises used, in particular security measures concerning the physical protection of security zones where ICT system assets or data storage media are located.

16.2. At the same time, the Supplier undertakes to ensure the physical security of installation, backup, and archival media and related documentation, including their labeling, storage, disposal, and maintenance of relevant records, in accordance with the Client's asset classification, provided the Supplier has been made aware of it.

17. Security Tools

17.1. The Supplier undertakes to implement security measures to remove or block network connections that do not comply with the requirements for protecting the integrity of the communication network. At the same time, the Supplier shall ensure that access from mobile devices to the Client's environment takes place exclusively via a secure VPN connection or another adequate technical measure.

17.2. Only network devices that have undergone an approval process and have been expressly authorized by the Customer may be connected to the Customer's environment. All unused network terminations and unused ports of active network elements managed by the Supplier must be deactivated immediately.

18. Use of Tools and Protection of Equipment

18.1. The Supplier undertakes not to install on the Customer's assets or use in the Customer's environment any tools that are not part of the services provided, in particular:

a) keylogger – software or hardware that unauthorizedly records keystrokes with the aim of compromising the confidentiality of entered data and information.

b) sniffer – software or hardware that enables the interception of network traffic.

c) vulnerability scanner – a software or hardware tool enabling the search for vulnerabilities in ICT systems, the detection of available network services and ports, running processes, running applications, and their versions.

d) backdoor – a hidden software or hardware tool that allows bypassing approved authentication procedures, installed with the aim of facilitating future unauthorized access to the ICT system

e) malware or other malicious software that disrupts, bypasses, or otherwise restricts security measures in the Customer's environment.

18.2. Only ICT devices protected against malware and other malicious software may be connected to the Customer's environment, provided their technology permits it.

19. Data Monitoring and Retention

19.1. The Supplier is obligated to continuously record and store operational and location data of ICT devices in accordance with the requirements of Czech and European legislation, ensure the collection of information on operational and security activities, and protect this information from unauthorized access or alteration.

19.2. Upon request, the Supplier shall provide the Customer with reports containing the results of monitoring user and administrator activities as well as other events within the scope of the subject matter of performance for the entire duration of the Contract.

20. Encryption and Communication

20.1. The Supplier further undertakes to ensure that online transactions carried out via web technologies take place through encrypted communication using the highest available version of the TLS protocol and corresponding certificates to ensure the confidentiality, integrity, and identity of the communicating parties.

20.2. All non-public information provided by the Client must be protected by appropriate encryption and secured against unauthorized access, particularly when used on mobile devices.

21. Liability and Monitoring

21.1. The Supplier acknowledges that, unless otherwise specified in the contract, a technical connection that disrupts the operation of the Customer's services may be terminated immediately without prior notice.

21.2. The Contractor further acknowledges that all of its activities and performance carried out on the Client's premises are monitored and evaluated within the scope of the subject matter of the contract and in accordance with the Client's internal documents, with which the Contractor has been familiarized.

Požadavky na kybernetickou bezpečnost dodavatelů

1. Systém řízení bezpečnosti informací

1.1. Dodavatel se v rámci poskytování služeb zavazuje uplatňovat bezpečnostní zásady a procesy zajišťující ochranu dat a informací vytvářených a zpracovávaných při poskytování služeb. Na základě bezpečnostních potřeb a výsledků hodnocení rizik je povinen zavádět odpovídající bezpečnostní opatření, průběžně je monitorovat a vyhodnocovat jejich účinnost.

1.2. Dodavatel se dále zavazuje vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaných služeb, zaznamenávat všechny podstatné okolnosti související s jejich zabezpečením a tyto záznamy na vyžádání zpřístupnit Objednateli.

1.3. Současně je povinen stanovit a udržovat aktuální bezpečnostní opatření ve formě procesů a technologií, které zajišťují plnění bezpečnostní politiky.

2. Řízení rizik

2.1. Dodavatel se v rámci poskytování služeb zavazuje řídit vlastní rizika, která mohou ovlivnit jejich poskytování.

3. Organizační bezpečnostní požadavky

3.1. Dodavatel se v rámci poskytování služeb zavazuje zejména k následujícím povinnostem:

a) nejpozději do 5 dnů od uzavření Smlouvy jmenovat odpovědnou kontaktní osobu pro účely zajištění plnění těchto požadavků na kybernetickou bezpečnost a související komunikace mezi smluvními stranami (dále jen „Kontaktní osoba“) a ve stejné lhůtě písemně oznámit její údaje Objednateli. Určení Kontaktní osoby pro oblast kybernetické bezpečnosti na straně Dodavatele se nedotýká ustanovení Smlouvy o pověřených osobách;

b) zajišťovat poskytování služeb výhradně prostřednictvím oprávněných osob, které byly řádně obeznámeny s příslušnými ustanoveními interních předpisů Objednatele a které disponují ověřenou kvalifikací, znalostmi a zkušenostmi nezbytnými pro řádné poskytování služeb.

4. Řízení subdodavatelů

4.1. Dodavatel se dále zavazuje:

a) zajistit dodržování požadavků na kybernetickou bezpečnost ve smluvních vztazích se svými subdodavateli, pokud jsou zapojeni do poskytování služeb. Současně je povinen do 10 dnů od účinnosti Smlouvy, na jejímž plnění se subdodavatelé podílejí, doložit Objednateli písemné prohlášení o jejich souladu s požadavky na kybernetickou bezpečnost;

b) uzavírat samostatné smlouvy se svými subdodavateli, zaměstnanci a dalšími osobami podílejícími se na plnění této Smlouvy, pokud je v rámci poskytování plnění zpracováváno osobních údajů, a to v souladu s příslušnými ustanoveními Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

5. Bezpečnost lidských zdrojů

5.1. Dodavatel se v rozsahu poskytování služeb zavazuje na vyžádání doložit Objednateli, že všechny osoby podílející se na poskytování služeb byly prokazatelně seznámeny s těmito požadavky na kybernetickou bezpečnost a s příslušnými ustanoveními interních řídících předpisů Objednatele, přičemž za prokazatelné seznámení se považuje zejména školení pracovníků Poskytovatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy.

5.2. Poskytovatel je povinen dodržovat příslušná ustanovení interních řídících předpisů Objednatele v rozsahu, v jakém byl s těmito předpisy seznámen, a v případě, že je součástí poskytovaných služeb služba dohledu, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu poskytovaných služeb.

5.3. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování služeb Objednateli v prostředí nebo s prostředky Objednatele:

a) využívaly pro ukládání a sdílení dat a informací výhradně k tomu schválené prostředky;

b) neukládaly ani nesdílely data a informace eticky nevhodného obsahu odporující dobrým mravům nebo poškozující jméno Objednatele;

c) nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové či spustitelné soubory v rozporu s licenčními podmínkami nebo právními předpisy v oblasti autorského práva;

d) nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

e) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;

f) nerealizovaly pokusy o neoprávněnou modifikaci či jiné neoprávněné zásahy do prostředků Objednatele, a to ani tehdy, pokud jim byl prostředek Objednatele svěřen do správy;

g) nepodílely se prostřednictvím prostředků Objednatele na šíření spamu či škodlivého softwaru.

5.4. Výše uvedené se vztahuje i na použití prostředků mimo prostředí Objednatele.

5.5. Dodavatel bere na vědomí, že podmínkou umožnění přístupu ke zdrojům Objednatele je zpracování osobních údajů pracovníků Dodavatele, kteří se podílejí na plnění předmětu Smlouvy. Nebude-li Objednateli umožněno takové osobní údaje zpracovávat, přístup ke zdrojům nebude umožněn.

6. Řízení provozu a komunikace

6.1. Dodavatel se zavazuje zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování služeb a dále zajistit, aby pro tyto účely byly využívány výhradně aplikace a technologie v souladu s platnou českou a evropskou legislativou, zejména s ohledem na licenční podmínky a autorský zákon.

6.2. Na vyžádání poskytne Dodavatel Objednateli přehled nebo report o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

7. Řízení změn

7.1. Dodavatel se zavazuje přiměřeně reagovat na změny ze strany Objednatele a odpovídajícím způsobem upravit svá technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

7.2. Dodavatel se dále zavazuje aktivně spolupracovat s Objednatelem při testování každé významné změny.

8. Řízení přístupu a oprávnění

8.1. Dodavatel se zavazuje přidělovat oprávnění svým pracovníkům pouze v rozsahu nezbytném pro výkon činností, a to tak, aby byla minimalizována rizika nežádoucího přístupu k prostředkům Objednatele. Udělený přístup nesmí být sdílen více osobami, ledaže to vyžaduje využívaná technologie; v takovém případě je Dodavatel povinen vést evidenci využívání sdílených přístupů a tuto evidenci na vyžádání předložit Objednateli.

8.2. Dodavatel dále zajistí, aby všechny osoby podílející se na poskytování služeb chránily autentizační prostředky a údaje a neposkytovaly neautorizovaný přístup dalším osobám. Současně je povinen průběžně kontrolovat a vyhodnocovat oprávněnost a nezbytnost přístupu všech osob, které mají přístup do prostředí Objednatele.

9. Zásady povolování a řízení přístupu

9.1. Dodavatel bere na vědomí, že přístup k systému ICT lze povolit pouze jeho zaměstnancům nebo zaměstnancům jeho subdodavatelů, a to na základě jeho požadavku.

9.2. Přidělení oprávnění zaměstnanci se řídí principem nezbytného minima a není nárokové. V případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a považován za bezpečnostní incident. V takovém případě mohou být uplatněny postupy zvládání bezpečnostních incidentů, včetně okamžitého zrušení přístupu k informačním aktivům Objednatele.

10. Implementace a dokumentace

10.1. Dodavatel se zavazuje zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění, a dále předat Objednateli dokumentaci obsahující zejména:

a) veškerá bezpečnostní nastavení, funkce a mechanismy;

b) popis autentizačního a autorizačního konceptu pro přidělování oprávnění;

c) instalační a konfigurační postupy.

11. Vývoj softwaru

11.1. Pokud předmět služby zahrnuje vývoj softwaru, zavazuje se Dodavatel:

a) dodržovat a implementovat nejlepší praktiky bezpečného vývoje softwaru stanovené smluvním vztahem;

b) na vyžádání umožnit audit provedeného nebo probíhajícího plnění a po jeho dokončení předložit vyvíjený kód a výstupy z code review, zejména za účelem ověření, zda plnění probíhá či probíhalo v souladu se Smlouvou a těmito požadavky na kybernetickou bezpečnost;

c) poskytovat přiměřenou součinnost při bezpečnostním testování v průběhu vývoje i po předání softwaru;

d) zajistit, aby plnění obsahovalo pouze objektivně nezbytné a smluvně sjednané součásti;

e) používat při instalaci operačních systémů či softwaru třetích stran aktuální verze produktů kompatibilních s prostředím Objednatele;

f) zajistit bezpečnost testovacího prostředí a ochranu testovacích dat;

g) dodat do produkčního prostředí pouze smluvně specifikovaný kompilovaný či spustitelný kód a nezbytná data pro jeho provoz;

h) garantovat, že dodávaný software bude v souladu s bezpečnostními politikami a standardy Objednatele, s nimiž byl prokazatelně seznámen, a že tento soulad bude otestován;

i) instalovat software výhradně na základě předem schválených migračních postupů;

j) nevyvíjet, nekompilovat ani nešířit v prostředí Objednatele programový kód, jehož účelem by bylo nelegální ovládnutí, narušení dostupnosti, důvěrnosti či integrity, anebo neautorizované či nelegální získání dat a informací.

12. Kybernetické bezpečnostní události a incidenty

12.1. Dodavatel se zavazuje stanovit a popsat činnosti, role a odpovědnosti nezbytné pro rychlé a účinné zvládání bezpečnostních incidentů. Dále je povinen bezodkladně hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálně negativním dopadem, a to prostřednictvím určeného komunikačního kanálu nebo Kontaktní osoby. Současně je povinen vyhodnocovat a uchovávat informace o incidentech v souladu s platnou českou a evropskou legislativou a poskytovat Objednateli aktivní součinnost včetně relevantních informací o podezřelých zařízeních či osobách.

12.2. Po dohodě s Objednatelem je Dodavatel povinen přijmout přiměřená opatření ke zmírnění dopadu incidentu nebo k jeho ukončení. Je rovněž povinen spolupracovat při analýze příčin incidentu a navrhovat opatření k zamezení jeho opakování, pokud incident způsobil nebo se na něm podílel

13. Odpovědnost Dodavatele

13.1. Dodavatel bere na vědomí, že bezpečnostní incident nebo jiné porušení požadavků na kybernetickou bezpečnost způsobené příčinou na jeho straně se nepovažuje za okolnost vylučující jeho odpovědnost za prodlení s řádným a včasným plněním předmětu Smlouvy a nezakládá právo na náhradu případné újmy Dodavateli ani třetí osobě ze strany Objednatele. Toto ustanovení není na újmu ostatním ujednáním Smlouvy o odpovědnosti Dodavatele za prodlení.

14. Kontinuita služeb

14.1. Dodavatel se zavazuje udržovat odpovídající kontinuitu svých aktiv nezbytných pro poskytování služeb. Současně se zavazuje pravidelně ověřovat a testovat svou schopnost tuto kontinuitu zajišťovat v souladu s dohodnutou úrovní služeb.

15. Kontrola a audit

15.1. Dodavatel se zavazuje v souvislosti s poskytováním služeb poskytovat přiměřenou součinnost při kontrolách prováděných Objednatelem nebo příslušnými úřady.

16. Fyzická bezpečnost

16.1. Dodavatel se zavazuje dodržovat provozní řády budov a využívaných prostor, zejména režimová opatření týkající se fyzické ochrany bezpečnostních zón, v nichž se nacházejí aktiva systémů ICT nebo datové nosiče.

16.2. Současně se zavazuje zajistit fyzické zabezpečení instalačních, záložních a archivních médií a související dokumentace, včetně jejich označení, uchovávání, likvidace a vedení příslušné evidence, a to v souladu s klasifikací aktiv Objednatele, pokud s ní byl seznámen.

17. Bezpečnostní nástroje

17.1. Dodavatel se zavazuje realizovat bezpečnostní opatření k odstranění nebo blokování síťových spojení, která nejsou v souladu s požadavky na ochranu integrity komunikační sítě. Současně zajistí, aby přístup z mobilních zařízení do prostředí Objednatele probíhal výhradně prostřednictvím zabezpečeného připojení VPN nebo jiného adekvátního technického opatření.

17.2. Do prostředí Objednatele smí být připojována pouze síťová zařízení, která prošla schvalovacím procesem a byla Objednatelem výslovně povolena. Všechna nevyužívaná zakončení sítě a nepoužívané porty aktivních síťových prvků ve správě Dodavatele musí být bezodkladně deaktivována.

18. Používání nástrojů a ochrana zařízení

18.1. Dodavatel se zavazuje, že na aktiva Objednatele nebude instalovat ani v jeho prostředí používat nástroje, které nejsou součástí poskytovaných služeb, zejména:

a) keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

b) sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

c) analyzátor zranitelností – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí.

d) backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT

e) malware či jiný škodlivý software, který narušuje, obchází nebo jinak omezuje bezpečnostní opatření v prostředí Objednatele.

18.2. Do prostředí Objednatele lze připojovat pouze zařízení ICT chráněná proti malwaru a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

19. Monitorování a uchovávání dat

19.1. Dodavatel je povinen průběžně zaznamenávat a uchovávat provozní a lokalizační údaje zařízení ICT v souladu s požadavky české a evropské legislativy, zajišťovat sběr informací o provozních a bezpečnostních činnostech a chránit tyto informace před neoprávněným čtením nebo změnou.

19.2. Na vyžádání poskytne Objednateli reporty obsahující výsledky monitorování uživatelských a administrátorských aktivit i jiných událostí v rozsahu předmětu plnění po celou dobu trvání Smlouvy.

20. Šifrování a komunikace

20.1. Dodavatel se dále zavazuje zajistit, aby on-line transakce realizované prostřednictvím webových technologií probíhaly prostřednictvím šifrované komunikace využívající nejvyšší dostupnou verzi protokolu TLS a odpovídající certifikáty k zajištění důvěrnosti, integrity a identity komunikujících stran.

20.2. Veškeré neveřejné informace poskytnuté Objednatelem musí být chráněny vhodným šifrováním a zabezpečeny proti neautorizovanému přístupu, zejména při používání na mobilních zařízeních.

21. Odpovědnost a monitorování

21.1. Dodavatel bere na vědomí, že technické spojení narušující provoz služeb Objednatele může být, pokud smlouva nestanoví jinak, okamžitě ukončeno i bez předchozího upozornění.

21.2. Dále bere na vědomí, že veškeré jeho aktivity a plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předmětu plnění a v souladu s interními dokumenty Objednatele, s nimiž byl seznámen.