Information Security and Data Protection Corporate Rules

1. These Information Security and Data Protection Corporate Rules (hereinafter referred to as "Rules") are applied to the contractual relationships between the company T-Mobile Czech Republic a.s. (hereinafter “TMCZ”) and the other party (hereinafter the "Contractor" or “Supplier”), arising from their business activities, including in particular purchase orders issued by TMCZ and any other agreements entered into between TMCZ and the Contractor (hereinafter the "Agreement") whose subject matter is in particular the supply of movable property (goods), construction work and/or provision of services or any other performance (hereinafter the “Activities”) by the Contractor of TMCZ (hereinafter referred to as “Performance”).

2. When providing Performance according to the Agreement the Contractor undertakes to comply with the requirements of the following international standards:

Implemented	Certified	System
Yes	Yes	Quality management system according to ISO 9001
Yes	Yes	Environmental management system according to ISO 14001
Yes	Yes	Information security management system according to ISO 27001
Yes	Yes	Continuity management system according to ISO 22301
Yes	Yes	IT service management system according to ISO 20000-1

3. The Contractor undertakes to provide Performance under the Agreement and to ensure performance of Activities to which they are committed under the Agreement, primarily through its employees. In case the Contractor will use Subcontractor, such Subcontractor must be approved by TMCZ and must be named in Appendix No. 3 of these Rules and/or Agreement, unless the Contractor and TMCZ agreed otherwise. Unless the Contractor and TMCZ have expressly agreed otherwise, the Contractor is not entitled to entrust any Subcontractor to perform its obligations under the Agreement without the prior written consent of TMCZ.

4. If TMCZ permits to the Contractor the use of a particular Subcontractor, the Contractor is obliged to conclude with such Subcontractor agreement that will ensure that the Subcontractor performs the obligations under the Agreement under the same conditions and quality as agreed between TMCZ and Contractor in the Agreement so that compliance with TMCZ requirements defined by the Agreement is ensured. The Contractor is fully responsible for the proper and timely fulfilment of these obligations by the Subcontractor. In particular, but not exclusively, such a Subcontractor must commit itself to respecting all the requirements and obligation of Contractor according to these Rules. In particular, the terms and conditions of access, rights and obligations to ensure the protection of any technical, commercial or other information (“Confidential Information”) that the Contractor has become aware of during the term of the Agreement, regardless of whether they are marked as confidential. The obligation to ensure confidentiality survives any expiration or termination of the Agreement.

5. In case that the Contractor has implemented or certified system, which is mentioned in section 2 of these Rules, then it must submit to TMCZ documented information (e.g. documents, records, logs) related to the requirements of the aforementioned systems for inspection and control, in order to demonstrate compliance with the requirements defined by the aforementioned international standards and the Agreement. If the Contractor provides Performance under the Agreement with the assistance and/or by the approved Subcontractors who have one of these systems implemented and certified, the Contractor shall ensure such

Subcontractors´ consent to carry out the audit of these Subcontractors in order to verify conformity with the aforementioned international standards.

6. If the Contractor does not have any system certified or implemented, it agrees to carry out audits aimed at verifying compliance with the requirements of the Agreement. Contractor is obliged to provide TMCZ employees or authorized persons with necessary cooperation to carry out the audit and risk analysis, submit for inspection and control any documented information (e.g. documents, records, logs), and is further obliged to allow access to premises and systems related to Performance according to Agreement. If the Contractor provides Performance with the assistance and/or by approved Subcontractors who do not have any of the systems implemented or certified, the Contractor will ensure such Subcontractors´ consent to the audit of these Subcontractors in order to verify conformity with the Agreement.

7. The Contractor and its Subcontractors shall, within agreed deadlines, undertake activities and/or implement corrective actions which have been identified and agreed upon as the outcome of the Contractor's audits. Likewise they are required to perform activities and implement corrective actions identified for example in tests, exercises, incidents, risk management. The Contractor shall provide TMCZ with all information (e.g. audit reports) relating to the ability of the Contractor to provide Performance according to the Agreement. If the implementation of the corrective measures lasts for more than 30 days, unless otherwise agreed in a specific case and/or the correction plan is not approved by the Contractor or such a plan does not provide a remedy and the Contractor does not notify reservations about the proposed corrective measures within the specified period, such situation shall automatically be considered as material breach of the Agreement and TMCZ is in such case entitled to withdraw from the Agreement. In the event that a request for the implementation of a corrective measure is made by a competent state authority in accordance with applicable law, or the implementation of a corrective measure is necessary due to compliance with legal obligations of TMCZ or the need to resolve a security incident, the Contractor is obliged to provide the required cooperation within the period specified by TMCZ, its non-provision is considered a material breach of the Agreement with the right to withdraw from the Agreement.

8. The Contractor shall have a business continuity management system in place to be able to provide to TMCZ performance under the Agreement in case of non-standard and unexpected situations continuously and in accordance with parameters and quality agreed between the Parties. The Contractor is obliged to provide TMCZ with cooperation in the preparation and implementation of business continuity or disaster recovery plans in TMCZ. Contractor is obliged to meet the requirements for business continuity management specified in Appendix No. 2 of these Rules in case when Performance according to Agreement will be evaluated according to business impact analysis (BIA) as critical and/or there is a legal reason for managing the Contractor in the area of business continuity management (BCM).

9. Contractor is obliged to dispose of the waste that originated from the Contractor or of which the Contractor is owner in connection with the Performance under the Agreement, in accordance with generally binding legal regulations, in particular those governing the area of waste management.

10. Employees, staff, delegated persons and Subcontractors of the Contractor (hereinafter the "Designated Persons") entering the premises or buildings of TMCZ and performing there Activities under the Agreement are required to familiarize themselves with the documentation of safety and health protection at work, about the fire protection and fire-fighting equipment located in the premises of the relevant TMCZ building.

11. The Contractor undertakes according to applicable fire protection regulations to:
    a) comply with applicable and binding fire protection regulations,

b) abide by the rules of fire safety specified in regulations of TMCZ objects and premises,
c) ensure the participation of the Designated Persons in training on fire protection if its Designated Persons are staying in TMCZ buildings and premises.

12. The Contractor undertakes within the fulfilment of the Agreement to comply with all generally binding legal regulations and other applicable regulations (e.g. CTN) to ensure safety and health protection at work.

13. The Contractor shall ensure that the Designated Persons comply with the applicable regime, technical and organizational measures governing the entry, movement of persons and means of transport in the premises and buildings of TMCZ. In order to allow persons and/or vehicles to enter the premises and buildings of TMCZ, the necessary permits will be issued to the Contractor by the relevant TMCZ department. The Contractor shall apply for authorization through a contact person pursuant to section 22 and 23 of these Rules.

14. TMCZ responsible person is responsible for familiarization of Designated Persons of Contractor with the relevant TMCZ internal regulations and handover of Access Means to Designated Persons.

15. The Contractor acknowledges that Designated Persons shall be inspected in accordance with TMCZ internal regulations (e.g. physical inspection of persons and means of transport, technical inspection of equipment) at the entrance to TMCZ premises. Designated Persons carrying out activities in TMCZ premises are obliged to identify themselves before entering the premises (e.g. an employee card, identity card, passport).

16. If Access Means to the premises or objects of TMCZ are handed over to the Contractor, the Contractor shall observe TMCZ´s internal regulations concerning the Access Means. The Contractor may not make a duplicate or a copy of the Access Means.

17. Contractor and Designated Persons are entitled, when providing the Performance under this Agreement, to reside and move in premises and buildings of TMCZ only for the time required for the performance of agreed Activities and Services, and only in premises and buildings, which are designated for those Activities.

18. Contractor and TMCZ acknowledge and agree that all information contained in the Agreement as well as follow-up contracts and information exchanged between TMCZ and the Contractor in connection with the providing of Performance under the Agreement will be kept confidential and protected to the extent of the terms agreed in the Agreement and/or non-disclosure agreement between TMCZ and the Contractor (hereinafter the "NDA") and / or any other related specific agreement governing the conditions for the protection of information (e.g. in the field of personal data protection, cyber security, etc.) (hereinafter the “Special Agreement”). Unless otherwise agreed, in case of contradiction between terms of NDA and Agreement, terms of the Agreement shall prevail and in case of contradiction between the Agreement and the Special Agreement, the provisions of the Special Agreement regarding the conditions of protection of information shall always prevail.

19. The Contractor undertakes to create, use and maintain adequate technical, organizational and personal security measures to ensure confidentiality, availability and integrity of Confidential Information which have been or will be provided or made available to the Contractor by TMCZ or its business partners. These measures must be sufficient to prevent the accidental or unauthorized destruction, loss, confusion, disclosure or any unauthorized forms of exploitation of Confidential Information. The Contractor shall maintain these measures in operational condition throughout the entire period of use of the Confidential Information.

20. When providing the Performance under the Agreement, the Contractor is responsible that the Performance will be delivered without defects, with due skill and care and in accordance with the requirements set out in the Agreement and the Annex No. 1 of these Rules.

21. The Contractor represents that Performance under the Agreement will be supplied only by the employees who, related to the nature of Performance, have a clean criminal record and are meeting the necessary qualifications and that the Contractor is capable upon TMCZ´s request to prove this. This obligation shall apply also to Subcontractors, who will participate in the provision of Performance on behalf of the Contractor.

22. The Contractor must ensure protection of the confidentiality and integrity of all access means (access ID, passwords, tokens, smart cards, access cards, keys etc.) into electronic systems and premises of TMCZ (in these Rules also the "Access means"), which are made available under the Agreement to Contractor, and may not make them available to third parties. The Contractor shall immediately notify TMCZ about loss, theft, misuse or destruction of Access Means in accordance with section 28 of these Rules.

23. The Contractor undertakes to instruct its Designated Persons that they are required to:
    a) use only the main entrance to enter and exit TMCZ premises; other entrances and exits can only be used in exceptional situations (e.g. evacuation, carry of excessive cargo),
    b) where required, without prompting to show ID card at the entrance to the premises to the authorised employee and/or authorised person of TMCZ,
    c) ensure that the data (if required) stated on the Access Means correspond to reality;
    d) protect the Access Means from damage, destruction, loss, theft and misuse by another person,
    e) not to provide the Access Means to other persons,
    f) if assigned, visibly carry the visitor's card for the whole period of stay in TMCZ,
    g) immediately notify TMCZ of any loss, theft, damage, misuse of the Access Means, including any changes to the data contained on the Access Means,
    h) to prove its identity by using the Access means based on the request of TMCZ employee,
    i) not allow any person to enter TMCZ building,
    j) upon performance of the agreed Activities, to return the Access Means, as well as any other items belonging to TMCZ.

24. Contractor and all persons involved in the provision of Performance under the Agreement on its behalf, are obliged to adhere to and comply with the established security measures of TMCZ and security instructions of TMCZ and are not allowed to perform any actions that might disturb these measures or damage them.

25. The Contractor is obliged to always inform TMCZ if any of the Designated Persons ends their employment (supplier) relationship with Contractor and at the same time is obliged to return to TMCZ all Access Means that TMCZ has provided to such person. In case of loss of Access Means, the Contractor shall be obliged to compensate TMCZ for any damage incurred.

26. Confidential data with a large volume will be exchanged between TMCZ and Contractor only in such a way that will guarantee the confidentiality and integrity of transmitted data (e.g. transfer using SFTP protocol with files which have pre-determined type and format).

27. TMCZ and the Contractor will establish a common point of contact for resolving all problems, mutual information sharing, cooperation in the field of information security and data protection and for such purpose will delegate contact employee. In the event of a change of this person, the Contractor undertakes to immediately delegate a new contact person and notify TMCZ of its contact information.

28. The Contractor is obliged to notify TMCZ immediately of any nonstandard situation, suspicious events, security incidents and loss of the Access Means, through the following contacts: email: security@t-mobile.cz, phone: +421 800 100 166.

29. The Contractor shall, within providing of Performance to TMCZ, make every effort to prevent the continuation of the security incident, to prevent further security incidents, to secure and restore all measures necessary to protect TMCZ's data and information.

30. If the Performance of the Agreement involves the performance of Activities directly related to (a) Contractor ensures the functionality of the technical and software means forming TMCZ information and/or communication system and/or (b) such relationship is relevant to TMCZ information and/or communication system and the Contractor thereby fulfilled the features defined in Czech Act No. 181/2014 Coll., on Cyber Security and in Czech Decree No. 82/2018 Coll., on Cyber Security, TMCZ and Contractor are obliged to conclude a service level agreement in the cyber security area before commencing these Activities.

31. Unless the Contractor and TMCZ expressly agree otherwise in the Agreement or any other separate agreement, the Contractor shall not have, within the scope of provided Performance according to the Agreement, access to:
    a) any personal data of TMCZ customers or employees according to the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and the Czech Act No. 110/2019 Coll. on Protection of Personal Data, as amended, and
    b) any data of the TMCZ customers or employees, which are subject of telecommunications privacy according to Czech Act No. 127/2005 Coll. on Electronic Communications, as amended.

32. Contractor is obliged to ensure that computer program (source and object code), which will be supplied to TMCZ within Performance, will contain only code developed in accordance with the requirements of the Agreement, the requirements of Annex No. 1 of these Rules and in accordance with the applicable standards under section 2 of these Rules. In particular, the Contractor undertakes that the code shall not contain any malicious and/or harmful features or security vulnerabilities that would impair the security of the Performance, and that it shall not contain any malware (as defined below). The Contractor is obliged to ensure protection against malicious codes and malware.The Contractor shall manage access to the code, limit it to the necessary circle of authorized persons and protect it against unauthorized manipulation.

33. Malware means, in particular, any computer program, set of commands and instructions used directly or indirectly in a computer with the ability to damage, interfere, disrupt and/or adversely affect the software, computer programs, data files and/or operation of any hardware, mobile and other terminal devices and/or network functionality, including viruses, worms, trojans, spyware, back doors and other programs that intentionally perform any unnecessary, disruptive and/or destructive functions within the information system.

34. Unless TMCZ and the Contractor agree otherwise, the Contractor undertakes to ensure:
    a) to use separately developed anonymised test data for development and testing purposes,
    b) separate development and testing environment separate from the live operating system,

c) prompt, safe and demonstrable destruction of test data upon completion of the need for their use,
d) before handing over the Performance under the Agreement, realisation of acceptance tests, which also includes security tests.

35. In case of breach of any obligation under these Rules, TMCZ shall be entitled to require the Contractor to pay a contractual penalty of 100,000 EUR (in words: one hundred thousand euro), for each individual case of breach. The contractual penalty is payable on the basis of an invoice issued by TMCZ without undue delay after breach of the respective obligations, within 14 days of its issuance. The Contractor undertakes to pay the contractual penalty duly and on time. Payment of the contractual penalty shall not affect the claim for damages exceeding the contractual penalty.

Annex No. 1 - Information Security Annex

GENERAL PRINCIPLES

This Information Security Annex (ISA) establishes the information security measures of T-Mobile Czech Republic a.s. which are members of Deutsche Telekom Group (DT). If applicable to the Deliverables listed in the Agreement, the Supplier must consider these measures as a minimum of security standard and they must apply for the duration of the Agreement, regardless whether the Deliverables are procured by the Agreement or via third party distributors.
These measures cover different aspects of information security and some are applicable depending on the nature of the Deliverables concerned by the Agreement.
In addition, these measures may be reinforced with additional security measures which will be provided by the Purchaser and agreed between the Parties in documents attached to the Agreement, a NPA and/or an Order, or any other related contractual agreement that will follow the subsequent security measures (eg a contract entered into under the Cyber Security Act).

PRIORITY OF DOCUMENTS

This ISA is a standard document that applies to any and all Agreements entered into with the Supplier that make reference to this ISA.

The following shall apply:

1. The Agreement shall prevail over the ISA, unless a different order of precedence has been set out in the Agreement.; and
2. Notwithstanding the above, all terms written in capital letters shall be interpreted according to the definitions at the end of this ISA and by default as defined in the Agreement containing the reference to this ISA.

The Parties agree that this ISA shall further prevail over Supplier documents defining security measures attached to or referenced in the Agreement, a NPA and/or an Order.

GENERAL APPLICABILITY OF ISA

The Supplier shall comply with ISA requirements for all Deliverables as defined in the following:

- **Software** refers to off-the-shelf vendor (standard) software and/or custom software resulting from a Statement of Work mutually agreed by the Parties (e.g. Software Result),
- **Hardware** including any embedded software/firmware (e.g. end-user equipment and devices for Internet of Things, IT equipment, etc.),
- **XaaS/Cloud Services** (e.g. Software as a Service),

- **Professional/ Expert Services** for performing installation, training, integration, maintenance and/or consulting, and
- **Contractor's performances, which are subject to the requirements of the Cyber Security Act** as amended and represent performances relating to elements and information systems that are an components of the Purchaser´s critical infrastructure and / or directly related to the availability, confidentiality and integrity of Purchaser's networks and information systems as a provider of a basic service (hereinafter also referred to as " **Services related to the cyber security** ").

GENERAL APPLICABILITY OF SPECIFIC SECTIONS REGARDING THE DELIVERABLES

The following sections are applicable to any kind of Supplier Deliverable:

- **Section A: "**Contractual and standards compliance"
- **Section B: "**Security organization"
- **Section C: "**Incident management**"**

The following sections apply according to the nature of Deliverables as defined in table A:

- **Section D:** "Cryptography and authentication"
- **Section E:** "Security by design"
- **Section F:** "Software Vulnerabilities fixing"
- **Section G:** "Purchaser Data in XaaS/Cloud Services, Services related to the cyber security"
- **Section H:** "Access control of XaaS/Cloud Services, Services related to the cyber security"
- **Section I:** "Operations of XaaS/Cloud Services, Services related to the cyber security"
- **Section J:** "Access to and use of Purchaser systems and resources"
- **Section K:** "Professionals and security"

Deliverable	Applicable sections
Software	**A, B, C, D, E, F**
Hardware	**A,B, C, D, E, F**
XaaS/Cloud Services	**A, B,C, D, E, F, G, H, I**
Professional/ Expert Services	**A, B, C, J, K**
Services related to the cyber security	**A, B, C, D, E, F, G, H, I, J, K**

Table A: Applicability of ISA sections

NON-COMPLIANCE WITH THIS ISA

If the Contractor becomes aware of a non-compliance with security measures specified in this ISA in his Deliverables, then the Contractor shall promptly submit to the Purchaser a situation analysis and a plan for remedy. If the Purchaser Approves the Remediation Plan, it shall be implemented by the Contractor at no cost to the Purchaser and the Supplier shall provide evidence of the effectiveness of the Remediation Plan.

If the non-compliance persists for more than 30 days, unless otherwise agreed in a particular case and / or the remedial plan is not approved by the Contractor or the plan fails to remedy, such condition will automatically be considered a material breach of contract where the Purchaser is in such authorized to withdraw from the Agreement.

A CONTRACTUAL AND STANDARDS COMPLIANCE

A.1 Security assessment of Deliverables

Upon request of the Purchaser, the Supplier shall provide the Purchaser within 10 working days all necessary information to assess the security of Deliverables such as security test/audit reports, vulnerability scans and code robustness analyses. If the Supplier provides the Purchaser with Services related to cyber security, it is obliged to provide the Purchaser with all necessary information, interoperation and cooperation.

A.2 Security policies

The Supplier shall apply an enterprise information security policy according to ISO/IEC 27001 standard or similar industry-recognized practice.

If the Supplier is certified, he shall provide the Purchaser with his security certification and keep him informed of renewals or revocations of his certificates.

If the Supplier was selected by the Purchaser based on a certification (e.g. ISO/IEC 27001), the Supplier shall maintain such certification during the entire term of his contractual duties.

A.3 Audit

The Purchaser shall have the right to undertake audits to check Supplier's compliance with the Purchaser's security requirements as defined in the Agreement.

A.4 Third Parties

In case the Supplier uses Third Parties in providing the Deliverables to the Purchaser, the Supplier shall ensure that such Third Parties meet the organizational and technical security measures agreed in the Agreement.

B SECURITY ORGANIZATION

B.1 Structure

Upon request of the Purchaser, the Supplier shall provide information about his security organization, including the cyber security management system if this obligation applies to the Supplier.

B.2 Point of contact

The Supplier shall nominate both a contact person for security related matters, reporting incidents or other events and an upper-management contact or key-account manager to handle escalation matters. The contacts shall be provided for each Order and changes shall be communicated promptly.

B.3 Security reviews

Once a year, upon request of one or both Parties, the Supplier and the Purchaser shall organize a meeting to review security aspects (e.g. evolutions and scheduled operations that may impact security).

Each Party can ask for an exceptional security meeting that shall be accepted by the other Party if the situation imposes a common analysis or immediate decision (for example a major incident or a significant evolution of threats).

B.4 Security measure for Purchaser data

The Supplier shall implement and comply with security measures according to the level of classification of the Purchaser's data.

The Supplier shall implement the following measures on classified Purchaser´s data :

- all data shall be encrypted when stored and transmitted,
- only authorized persons will have access to the processed data, and
- a strong authentication system (e.g. two-factor authentication system) shall be implemented.

The Parties shall agree in advance on a method of exchange in case of a need to exchange encrypted information. The Supplier is obliged to process the Purchaser's data through the established system of identity and access rights management. The supplier is also obliged to manage all privileged accesses and exceptions from the process of managing identities and access rights.

C INCIDENT MANAGEMENT

C.1 Detection

The Supplier shall have measures in place to detect and manage security incidents impacting the Purchaser and occurring in the Supplier’s environment. Security incidents include but are not limited to loss, alteration, disclosure or unauthorized access to Purchaser data or information and unauthorized disclosure of proprietary source code as well as cyber security incidents under the Cyber Security Act.

C.2 Notification

The Supplier shall promptly notify the Purchaser in case of any such security incident including all matters affecting the provision of cyber security.
Where breach and/or misappropriation of Purchaser’s data or information are determined, the Supplier shall notify the Purchaser according to applicable laws, but without any delay.
Details of security incidents shall be retained by the Supplier according to applicable laws , at least until the next security review between the Parties.

C.3 Resolution

The Supplier shall use best efforts to immediately resolve security incidents and inform the Purchaser of progress and end-of-incident including taking corrective action.

C.4 Suspension of Supplier access to Purchaser systems

NOTE: This paragraph C.4 is not applicable to XaaS/Cloud Services.

In the event of a security incident, the Purchaser may suspend Supplier access to Purchaser systems until the incident is resolved.

C.5 Suspension of Purchaser access to Xaas/Cloud Services

NOTE: This paragraph C.5 is not applicable to Software, Hardware Deliverables, Professional Services and Services related to the cyber security.

In the event of a security incident concerning XaaS/Cloud Services (e.g. system intrusion, malware incident), the Purchaser may suspend his access to the said Service until the incident is resolved.

In the event where the Purchaser is not able to suspend access, the Purchaser shall explicitly request the Supplier to suspend all Purchaser access until the incident is resolved. Supplier shall promptly comply with such request.

C.6 Security report

The Purchaser may request from the Supplier a security report related to the provided Services no more than twice a year; this does not affect the right of the Purchaser to request the necessary information at any time, if needed in connection with the fulfillment of legal obligations of the Purchaser. This security report shall include but is not limited to the following information:

- the number of security incidents detected over the last 12 months, separately for internal and external causes if relevant,
- details of security incidents over the period (detection time, nature and impact, resolution, service recovery time, closing time, time for resolution), and
- all information that the Purchaser will request in connection with the fulfillment of its legal obligations and requirements, in particular in connection with the applicable legislation in the field of cyber security and privacy.

D CRYPTOGRAPHY AND AUTHENTICATION

D.1 Modification of authentication data and cryptographic keys by Purchaser

All authentication data and cryptographic keys (e.g. certificates, key pairs, symmetric keys, passwords) in Software, Hardware Deliverables and Services related to the cyber security shall be modifiable by the Purchaser and protected according to state-of-art. For authentication data and cryptographic keys that are not modifiable by the Purchaser, Supplier shall provide a list of such data and their purpose to Purchaser. For XaaS/Cloud Services, this requirement applies only to authentication data used by the Purchaser for protecting its data.

D.2 Strength of cryptographic algorithms and keys

The Supplier shall implement only standardised cryptographic algorithms recommended by governmental institutions (such as BSI, ANSSI and NIST) at the time the Agreement is agreed or renewed.

E SECURITY BY DESIGN

E.1 Hardening

The Supplier shall employ standardized system hardening practices. This includes restricting protocol access, removing or disabling unnecessary software, network ports and services, removing unnecessary files, user accounts, restricting file permissions, patch management and logging.

The Supplier shall provide Deliverables (including Third Party components and services) that are securely configured by default according to state-of-the-art security configuration practices (such as https://www.cisecurity.org/).

Notwithstanding the above, the Supplier shall provide the Purchaser with all necessary information to securely configure and use Deliverables and shall ensure that such information is always up-to-date during the term of the Agreement.

In addition, the Supplier shall ensure that Deliverables do not contain any Back Doors.

E.2 Testing for software security errors

The Supplier shall test the Deliverables to ensure that they are free of dangerous software errors listed in “CWE/SANS Top 25” (http://cwe.mitre.org) and/or “OWASP TOP 10” (http://www.owasp.org) at the delivery date (e.g. robustness against unexpected inputs such as SQL Injection, predictable behaviour in overload situations, etc.).

E.3 Additional measures

Upon request of the Purchaser the Parties may mutually agree on additional security measures that Deliverables must satisfy.

These additional measures may be gathered in a document called “Security Statement of Compliance” and be included in the Agreement and/or in the NPA.

F SOFTWARE VULNERABILITIES FIXING

F.1 Detection

The Supplier shall have measures in place to continuously monitor external security advisory sources (such as cooperative security tests, external security research, open source and third party disclosure, ...) and track Vulnerabilities that could impact the Deliverables (including Third Party components).

F.2 CVE Standard

Where appropriate, each Vulnerability detected by the Supplier shall have a unique CVE identifier associated with a CVSS score (v2 or higher). Any alternative must be agreed in writing with the Purchaser.

F.3 Notifications

The Supplier shall promptly provide information to the Purchaser about each Vulnerability (with CVSS score greater or equal than 7.0) including Zero-Day impacting the Deliverables and its consequences (e.g. CVE if exists, CVSS score, affected components or services).

F.4 Service level agreement to fix Vulnerabilities

For each Vulnerability impacting the Deliverables, the Supplier shall:

- make all efforts to provide a Temporary Fix to the Purchaser according to the following table, and
- make the Official Fix available to the Purchaser according to the following table.

CVSS base score v2	**The maximum time to provide a Temporary Fix**	**The maximum time to provide the Official Fix**
7.0-10.0	7 (seven) calendar days	30 (thirty) calendar days
0-6.9	not applicable	6 (six) months

The time counter starts when the Vulnerability is detected, except for a Vulnerability located on Third Party components where the time counter starts when a fix is available.

F.5 Security maintenance of third party components

The Supplier shall ensure that Third Party components used within the Deliverables are security maintained during the period of maintenance or Service contracted by the Purchaser.

F.6 Security Defects

The Supplier shall accept for each Vulnerability impacting the Deliverables and detected by the Purchaser during the contracted period of maintenance and/or warranty period that the Purchaser can open a maintenance ticket to fix it. In addition to section F.4, the Supplier shall respect the maintenance conditions to correct the Defect related to the Vulnerability.

F.7 Exceptions

The Supplier shall employ commercially reasonable efforts to support the Purchaser to fix Vulnerabilities:

- in occasions requiring a faster response than the above table (e.g. press publication of Vulnerability in a Deliverable used by the Purchaser), and
- in the technical environment necessary to operate the Deliverables (e.g. operating system for a Software Deliverable).

F.8 Damages/Penalties for Vulnerability fixes

In addition to the remedies as a consequence of a material breach as set out in section **Error! Reference source not found.** "**Error! Reference source not found.**", the Purchaser may apply damages or penalties to the Supplier as per the sections "Damages" or "Penalties" of the Agreement.

In case of Vulnerabilities the following penalties scheme shall apply:

If the Supplier fails to provide a security Official Fix for Vulnerabilities with a CVSS score equal to 7 or greater than 7 as per the table defined in section F.4 " Service level agreement to fix Vulnerabilities", the penalties are calculated as follows:

A = V x N / 300

A: amount of penalties

V: V is the value of the Deliverables

N: number of calendar days exceeding the Official Fix deadline

F.9 Security-related maintenance

During the contracted period of maintenance and/or warranty period, the Supplier shall provide Software and Hardware Deliverables and future releases with all security patches. The latter may be either applied or provided at the same time as a separate bundle.

During the life cycle of the Deliverable, the Supplier shall provide to the Purchaser security patches as and when they are released, respecting the Vulnerability Fix times defined in section F.4.

The Supplier shall provide information (e.g. CVE, CVSS score) to the Purchaser about the Vulnerabilities that have been fixed in patches.

G PURCHASER DATA IN: XAAS/CLOUD SERVICES, SERVICES RELATED TO THE CYBER SECURITY

G.1 Limitation of use of Purchaser data

The Supplier shall use Purchaser data transmitted, processed, generated and/or stored in the XaaS/Cloud Service only to provide the said Service.

G.2 Segregation of Purchaser data

The Supplier shall enforce segregation of Purchaser data from data of other customers of the Supplier.

G.3 Purchaser confidential data

The supplier shall encrypt in transit and in storage all data that is classified by the Purchaser as confidential.

G.4 Supplier encryption mechanisms

In case the Purchaser uses an encryption mechanism provided by the Supplier to protect Purchaser data, the Supplier shall ensure that:

- such data shall be kept encrypted when stored and transmitted, and
- a strong authentication (e.g. two-factor authentication) is used for access to such data.

G.5 Logging of Purchaser data access and use

The Supplier shall:

- log access to and usage of Purchaser data, including by his employees and any appointed third parties, and
- retain such logs for the duration agreed in the NPA and/or Order including associated documents (e.g. Non-Disclosure Agreement or Data Processing Agreement) or otherwise, 6 months by default.

Extracts of retained logs shall be provided to the Purchaser on request.

G.6 Purchaser Data reversibility

Upon termination of the NPA and/or Order, the Supplier shall make available to Purchaser for retrieval all Purchaser data in a format and for a period of time mutually agreed beforehand with the Purchaser.

As per section **Error! Reference source not found.**, only encrypted connections shall be used for Purchaser retrieval of data unless exception agreed in writing by Purchaser.

At the end of the data reversibility period, the Supplier shall destroy all Purchaser environments and Purchaser data in a manner designed to ensure that they cannot be accessed or read.

The Supplier shall provide the Purchaser with a certification of destruction.

H ACCESS CONTROL OF: XAAS/CLOUD SERVICES, SERVICES RELATED TO THE CYBER SECURITY

H.1 Physical security

The Supplier shall provide physically secured facilities for both production cloud infrastructure and locations for remote operations.

Controls shall include at least:

- physical access requires authorization and is monitored,
- everyone must visibly wear official identification while onsite, and
- visitors must sign a visitor's register and be escorted and/or observed when on the premises,
- possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Supplier employment must return keys/cards.

H.2 System access control and password management

The Supplier shall control the Service systems by restricting access to only authorized personnel.

The Supplier shall enforce password policies on infrastructure components and cloud management systems used to operate the Supplier Service environment. The Supplier shall protect passwords using secure mechanisms such as digital vault.

The Supplier shall implement system access control, and accounting designed to ensure that only approved operations and support employees have access to the systems. System access control shall include system authentication, authorization, access approval, provisioning, and revocation for employees and any other Supplier-defined 'users'.

H.3 Review of access rights

Network and operating system accounts for Supplier employees shall be reviewed regularly to ensure appropriate employee access levels.

In the event of Supplier employee´s leaving the contractual project, the Supplier shall take prompt actions to terminate network, telephony, and physical access for such former employees.

H.4 Security Gateway

The Supplier shall utilize security gateways (e.g. firewalls, routers, proxies, reverse proxies) to control access between the internet and Supplier Services by allowing only authorized traffic.

Supplier managed security gateways shall be deployed to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address, as appropriate, in order to identify authorized sources, destinations, and traffic types.

H.5 Anti-malware controls

The Supplier shall employ anti-malware software to scan uploaded files. Malware definitions shall be updated at least daily.

H.6 Encryption and remote connections

For Purchaser access to and use of a XaaS/Cloud Service, only encrypted connections must be used unless exception agreed in writing by Purchaser.

The Supplier shall ensure that only authenticated and encrypted connections are used for Third Parties acting on behalf of the Supplier accessing remotely Purchaser data processed and/or stored in a XaaS/Cloud Service.

In all cases, the latest available browsers must be supported for connecting to Xaas/Cloud Services.

I OPERATIONS OF: XAAS/CLOUD SERVICES, SERVICES RELATED TO THE CYBER SECURITY

I.1 Penetration tests

The Supplier shall assess the security of the Provided Services using penetration tests at least on a yearly basis. The report and mitigation plan of such tests shall be shared with Purchaser.

Notwithstanding the above, the Supplier shall allow Purchaser to make penetration tests on his production environment.

I.2 Production data and environments

The Supplier shall not use production data for testing activities.

The Supplier shall separate development, testing and production environments (e.g. networks, data, applications, etc.).

I.3 Disaster recovery plan

The Supplier shall set up and maintain a disaster recovery plan and ensure that it is tested at regular intervals.

Backups will be securely deleted by the Supplier upon disposal.

I.4 Security-related maintenance

For any security patch that the Supplier intends to deploy on the Provided Services, the Supplier shall apply and test the security patch on a testing environment. Only after successful completion of testing on such environment, the Supplier will deploy the patch on the production environment.

I.5 Third Party services

The Supplier shall inform the Purchaser if Third Party services (e.g. data center services) are involved or planned to be involved in the provision of the Service.

J ACCESS TO AND USE OF PURCHASER SYSTEMS AND RESOURCES

This section will be applicable only if the Purchaser grants the Supplier access to and use of Purchaser systems for the performance of the Agreement.

J.1 Physical

If Purchaser provides access and/or interconnection equipment installed on Supplier premises, the Supplier shall ensure that:

- physical access control is applied to the technical area where such equipment is located, and
- physical access to such equipment is limited to those who need to access the equipment for the performance of the Agreement and duly authorised by the Supplier.

J.2 Purchaser Systems

The Supplier shall:

- access and use Purchaser's systems only to provide the Deliverables,
- ensure that access and data transfer are secured by using encryption and are not used to perform the attack and other inappropriate activities (e.g. for data transfer, check for malware),
- comply with the means of access and rules defined by the Purchaser (including Best practice rules) and provided to the Supplier beforehand (e.g. respect network addresses assigned by Purchaser, respect Purchaser responsive times for Purchaser Asset management, ...),
- in the case of using remote access to the Purchaser's systems, has obligation to comply with the rules, methods and procedures specified by the Purchaser,
- ensure that anybody acting on behalf of the Supplier who needs to use the Purchaser systems is duly authorised by the Supplier and identification information has been provided to the Purchaser and the list of acting (authorized) persons was continuously maintained and updated, and
- ensure that only duly authorised Supplier Resources are connected with the Purchaser systems.

J.3 Purchaser systems and applications

If the Purchaser provides accounts to the Supplier, the Supplier shall:

- promptly notify the Purchaser when an account is no longer required, and
- ensure that accounts provided for server communications are used only for that purpose.

J.4 Management and operation of the Purchaser's information and communication technologies

If the Supplier provides Services related to the cyber security of the Purchaser, the Supplier is obliged to:

- comply with the rules of interconnection of the Purchaser 's systems and transmission of electronic information,
- manage network security and infrastructure changes according to the Purchaser's rules and instructions,
- apply capacity management of systems and services according to the rules and instructions of the Purchaser, and

- use controlled cryptographic measures,
- have implemented a system of management of continuity of processes and activities and ensure compliance with the system of continuity management of the Purchaser.

J.5 Purchaser Asset management

If the Purchaser provides Assets to the Supplier, the Supplier shall keep track of such Assets and manage access to the Assets by using the appropriate classification of such Assets. The Supplier applies a similar approach also in the case of processing personal data made available by the Purchaser.
Upon termination of the Agreement, the Supplier shall return Purchaser Assets still in his possession. The Supplier is also obliged, upon termination of the contractual relationship, to grant, provide, transfer or assign all necessary licenses, rights or consents needed to ensure the operation of the basic service to the Purchaser, who is in the position of the operator of the basic service; this obligation of the Supplier shall remain in force even after the termination of the contractual relationship for at least five years after the termination of the contractual relationship, unless otherwise agreed.

K PROFESSIONALS AND SECURITY

K.1 Awareness training and education

The Supplier shall ensure that his employees and any Third Parties appointed to provide the Deliverables:

- possess appropriate security skills (e.g. to manage security incidents),
- are familiar with the content and the implementation of applicable security rules and carry out all activities in accordance with these rules, and
- observe confidentiality of all facts and information of the Purchaser and sign a declaration of confidentiality.

K.2 Purchaser specific security rules

If the Purchaser provides specific security rules for performing the Professional Services and Services related to the cyber security, the Supplier shall ensure that his employees and any appointed Third Parties are informed of such rules before the start of any tasks.

K.3 Subcontractors

If the Supplier plan to use a Subcontractors to fulfil the Agreement with the Purchaser, the Supplier might to do so only with prior consent of the Purchaser, Supplier shall specifically identify them as Subcontractors and ensure contractually undertake that the same due care will always be applied. Such due diligence applies to all subcontracting relationships, including the acquisition, development and maintenance of systems and applications.

K.4 Handling of sensitive Deliverables

Upon request of the Purchaser, the Supplier shall commit to use only security checked personnel, i.e. screened by national authorities, for handling of sensitive Deliverables prior to deployment in the Purchaser's Network, as well as for maintenance of sensitive Deliverables during the whole operational phase.

DEFINITIONS AND ABBREVIATIONS

Agreement	means any contract signed by Purchaser with the Supplier and containing the reference to this ISA
Assets	encompass primary and supporting assets as defined in ISO/IEC 27005.
Back Door	means a feature or defect of Deliverables that allows surreptitious unauthorized access to data
CVE	means Common Vulnerabilities and Exposures as defined in: http://cve.mitre.org/index.html
CVSS	means Common Vulnerability Scoring System as defined in http://www.first.org/cvss/
Defect	means any deviation of the actual quality of the Deliverable from the contractually intended quality, e.g. default, non-compliance of the Deliverables with their corresponding specification or their failure to perform in accordance with related documentation
Deliverables	mean any equipment, product and/or service and activities ordered on the main Agreement including all main- and ancillary obligations.
Information Security	means – in compliance with ISO/IEC 27001 and ISO/IEC 27005 - security in the scope of information processing and activities (primary assets) relying on technical (including, but not limited to IT, premises, facilities, networks) and non-technical assets (including, but not limited to supporting assets such as staff, partners, organizations, procedures, terms and conditions)
Internet of Things	means any connected devices or equipment for internet of things
NPA	means a contract concluded by an Affiliated Company of DTAG under a Frame Agreement of DTAG, as the case may be, concluded by Purchaser. NPA corresponds with the terms “Implementation Contract”, “Project Specific Agreement” and “Project Agreement”: any provision using the term “NPA” shall apply to those kinds of agreements as well
Official Fix	means that a complete Supplier solution is available to fix a Vulnerability, either by means of an official patch or an upgrade
Order	means a purchase order issued by the Purchaser. “Order” corresponds with the term “Purchase Order” in Agreements concluded by DTAG and its Affiliated Companies. Any provision using the term “Order” shall apply to “Purchase Order” in the same way
Purchaser	means T-Mobile Czech Republic a.s. and the DTAG Affiliated Company as party to the NPA or Order. “Purchaser” corresponds with the term “Ordering Party” in Agreements concluded by DTAG and its Affiliated Companies. Any provision set out for the Purchaser in this ISA shall apply to “Ordering Party” in the same way
Purchaser Network	means the network managed by the Purchaser and all related Purchaser Network access infrastructures necessary to ensure the communications between each party Resources
Purchaser Assets	mainly means information, processes, hardware, software, services belonging to the Purchaser and used for the purpose of providing the Deliverables
Software Result	means any software that is: (i) primarily based on and/or directed to the DTAG Requirements and/or Specifications provided by or exclusively for Purchaser, and/ or (ii) developed or implemented by Supplier under this Agreement (and/or any subsequent amendments) and/or any TSA and/or NPA and/or any Order, and which is not a background;

	which may or may not be protected by intellectual property rights, as well as any product or process resulting from it
Statement of Compliance	means an exhibit of Agreement with detailed technical security requirements on Deliverables
Statement of Work (SoW)	means a document defining project-specific activities, deliverables and timelines for the Supplier providing Deliverables and/ or Services to the Purchaser
Supplier Resources	means hardware, software belonging to and/or under liability of Supplier and used for the purpose of providing the Deliverables
Temporary Fix	means that there is an official but temporary fix available to fix a Vulnerability, including – but not limited to – temporary hotfixes, tools or workarounds
Vulnerability	means a weakness that reduces availability, integrity or confidentiality
XaaS	means anything delivered to users as a service including SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) or similar
Zero-Day	means an undisclosed vulnerability that hackers can exploit to adversely affect Deliverables. It is known as a "zero-day" (or “zero-hour” or “0-day” or “day zero”) because it is not publicly reported or announced before becoming active, leaving the Supplier with zero days in which to create patches or advise workarounds to mitigate its actions
Cyber Security Act	Czech Act No. 181/2014 Coll. on Cyber Security and on Amendments to Certain Acts, as amended, including related implementing regulations, and, where appropriate, other legislation that will replace it in the future

Annex No. 2 - BCM Requirements

1) In order to ensure the protection of TMCZ´s business, the Contractor shall establish and maintain an effective business continuity system in accordance with ISO 22301. This system shall also include regular testing of business continuity plans to ensure that in an emergency or crisis situation and immediately thereafter the Contractor will be able to continue to fulfil its obligations towards TMCZ.
2) The Contractor shall ensure a sufficient degree of resilience and renewability of the Performance so as to guarantee the achievement of the RTOs as set out in the Service Level Agreement (SLA) for each Performance provided.
3) During the so-called Transitional Phase of the Agreement the Contractor shall prove its ability to renew all provided Performances by producing appropriate BCM documentation, which will then be tested for accuracy and completeness.
4) The Contractor shall implement and maintain a risk management system (including risk identification, control and acceptance process) for the provided Performance and relevant platforms delivered.
5) The Contractor shall promptly notify TMCZ of any identified or potential risks relevant to the provided Performance.
6) The Contractor shall provide the TMCZ with a list of known risks related to all assets relevant to the provided Performance.
7) The Contractor shall perform a Business Impact Analysis (BIA) for the Performance and platforms provided and identify impacts and vulnerabilities according to the methodology agreed with TMCZ.
8) The Contractor shall create Business Continuity Plans, Disaster Recovery Plans and Crisis Plan or another similar document. TMCZ has the right to review the BCM documentation.
9) The Contractor is responsible for creating, maintaining and testing the BCM documentation to the extent of the Performance and platforms delivered. TMCZ will cooperate with the Contractor in this area. TMCZ shall verify the Contractor's readiness to meet BCM obligations through regular exercises.

10) The Contractor shall review the BCM documentation at regular intervals and with each significant change, but at least once a year for delivered Performance. Changes will be subject to approval by TMCZ.
11) The Contractor shall ensure that its relevant employees maintain awareness of the content of the BCM documentation on the subject of Performance, verify the correct understanding of the content of the documentation and conduct regular training and updates.
12) The Contractor shall ensure that sufficient trained employees are available in the event of an emergency.
13) The Contractor shall carry out testing of implemented business continuity system measures according to the requirements of the contract at least once a year for delivered Performance.
14) The Contractor shall cooperate with TMCZ in the agreed BCM exercises.
15) The Contractor shall inform TMCZ at least one month in advance if he is preparing BCM exercises and shall provide the TMCZ with a report on the results of the exercise after completion of the exercise.
16) TMCZ reserves the right to audit the business continuity system at the Supplier. TMCZ also accepts an audit of an independent audit authority if it relates to the subject of Performance.
17) TMCZ reserves the right to participate in its Disaster Recovery Exercise to verify the functionality of the Supplier's recovery plans.
18) TMCZ reserves the right to access to the supplier's BCM documentation.
19) The Contractor shall promptly notify TMCZ of the outsourced partner's identification data if the subject of the Performance or parts thereof is outsourced.
20) The Contractor shall require at least the same level of business continuity for its Critical Contractors as TMCZ requires.
21) The Contractor shall immediately (but not later than within 3 months) implement the necessary measures defined by the audit or arising from tests, exercises, failures, risk analysis, or change management process related to the subject of Performance.
22) The Contractor shall provide TMCZ with information and findings from the ISO 27001 and 22301 audit, in particular findings concerning the Contractor's ability to provide the Performance.
23) The Contractor shall promptly report to the TMCZ any security incidents that caused or may cause a failure of the Performance.
24) The Contractor and TMCZ shall agree rules and requirements for incident handling.

Annex No. 3 - Approved Subcontractors

Company (business name, company ID, registered office, registration in the Commercial Register)	Provided Performance	Implemented / certified system according to section 2 of the Rules
		Yes / No