STANDARD TERMS & CONDITIONS OF PURCHASE

CZECH REPUBLIC

ATTACHMENT A

SECURITY FOR CARRIER INFORMATION

The following provisions of this policy are incorporated into Carrier's Standard Terms & Conditions of Purchase which may be found at https://www.corporate.carrier.com/suppliers/terms-conditions/ (the "Terms") and any Agreement whenever the Seller will store Carrier Information. All capitalized terms used in this policy but not defined shall have the same meaning given to them in the Terms.

1. Seller will use commercially reasonable efforts to establish, maintain and comply with administrative, technical and physical safeguards that are designed to (*a*) protect the security, availability and integrity of Seller's network, systems and operations, the Services and the Carrier Information; (b) guard against Security Issues; and (c) satisfy the requirements for certification under ISO 27001. Seller will develop, implement and maintain a written security program, reasonably acceptable to Buyer that includes appropriate administrative, technical, organizational and physical safeguards, security awareness and security measures designed to protect Carrier Information from unauthorized access and use.

2. Seller agrees to install and implement security hardware, software, procedures and policies that will provide effective information security and are acceptable to Buyer. Seller agrees to monitor and update such hardware, software, procedures and policies to utilize improved technology and to respond to developing security threats in order to maintain a level of security protection, preparedness and resilience appropriate for the information involved and the then current state of security solutions. Upon request, Seller shall provide Buyer with any reports or results of any internal audit related to IT security performed by or on behalf of Seller during the term of the Agreement and/or Order or any audit reports issued, including but not limited to, under the SSAE 16 report or ISAE 3402.

3. Seller further agrees to:

3.1 Only collect, access, use, or share Carrier Information, or transfer Carrier Information to authorized third parties, in performance of its obligations under the Agreement and/or Order, in conformance with the provisions set forth in this policy, or to comply with legal obligations. Seller will not make any secondary or other use (e.g., for the purpose of data mining) of Carrier Information except (a) as expressly authorized in writing by Buyer in connection with Buyer's purchase of Services hereunder, or (b) as required by law.

3.2 Maintain and implement information security policies which address, at a minimum the following domains:

3.2.1 information security policy

3.2.2. organization of information security

3.2.3 asset management

3.2.4 human resourced security

3.2.5 physical and environmental security

3.2.6 communications and operations management

3.2.7 access control

3.2.8 information systems acquisition, development and maintenance

3.2.9 information security incident management

3.2.10 business continuity management

3.2.11 regulatory compliance

3.3 Provide Buyer with an index or similar summary of its policies sufficient to evidence to Buyer's reasonable satisfaction that each domain is addressed in a manner consistent with this Section. Seller shall provide Buyer with an updated index or summary, upon Buyer's request, and indicate any plans, including a timetable for implementation, of planned upgrades to comply with the policy. Seller shall implement those reasonable requests for modification of such policy requested by Buyer.

3.4 Allow Buyer or its designee to conduct a security audit at its facilities on one day's notice, and allow Buyer at any time to conduct (or have conducted) a network audit. If the Carrier Information is stored in a shared environment per the agreement of Buyer, then Buyer shall use a third party to conduct such audits. The audits shall include any facilities with Carrier Information including backup storage facilities.

3.5 Segregate all Carrier Information into a separate database only accessible by Buyer, and its agents and those employees and agents of Seller that require access to perform the Services or to maintain the equipment and the program on which it runs, unless otherwise agreed by Buyer. Logical segregation of data, if approved by Buyer, may be an acceptable alternative to this requirement. Seller shall use reasonable efforts, as measured by the available technology at the time, to prevent anyone other than its authorized employees and Buyer and its agents from accessing the Carrier Information.

3.6 Assure that all Carrier Information and applicable software is appropriately backed up and recoverable in the event of a disaster or emergency, and that Seller's disaster recovery plan (as may be otherwise required herein) shall incorporate such requirements.

3.7 Provide Buyer, at the time of signing this Agreement and/or Order, with a termination plan that addresses how Carrier Information will be returned to Buyer at the end of this Agreement and/or Order, including backup and archival information, and how all Carrier Information will be permanently removed from Seller's equipment and facilities. This plan should include supplying the data to Buyer in an industry recognized nonproprietary database and, if not, a license to use the proprietary database software to access the data.

3.8 Provide information to and fully cooperate with Buyer in response to any subpoena, investigation or the like seeking Carrier Information and provide information and assistance for Buyer to seek certification and the like relative to its information including information in the possession of Seller. Seller shall promptly notify Buyer upon the receipt of any request requiring that Carrier Information be supplied to a third party.

3.9 When requested by Buyer, Seller agrees to comply, within a reasonable period of time, with Carrier Information security policies as provided to Seller by Buyer.

3.10 Seller shall not provide Carrier Information to any other entity without the prior written approval of Buyer. A request for Buyer approval shall include agreement by Seller, and such other entity, that (i) all of the requirements of this provision are applicable to their performance and (ii) Buyer shall have the right to perform the audits described above.

4. Encryption Requirements. Seller will use, and will cause Seller Personnel to use, appropriate forms of encryption or other secure technologies at all times in connection with the Processing of Carrier Information, including in connection with any transfer, communication, remote access or storage (including back-up storage) of Carrier Information, as authorized or permitted under the Agreement and/or Order. Notwithstanding any provision to the contrary herein, Buyer Personal Information shall not be stored on any Seller mobile computing devices (e.g. laptop computers, PDAs (personal digital assistants), etc.)

5. Notification. Seller will provide to Buyer immediate written notice of (i) any failure to meet the then current standards for information security, and (ii) any and all reasonably suspected and/or confirmed Security Issues. Such notice will summarize in reasonable detail the impact on Buyer or any individuals affected by such Security Issue and the corrective action and remediation efforts taken or proposed to be taken by Seller. Immediately following any Security Issue or any other failure to meet information security standards, whether identified by Seller or Buyer, Seller will take steps to mitigate risks posed, consult in good faith with Buyer regarding remediation efforts, and undertake a remediation plan which Buyer determines in its sole but reasonable discretion, to be necessary, reasonable or appropriate under the circumstances commensurate with the nature of the Security Issue or failure, or as requested by any government body. Seller will be solely responsible for all costs and expenses, including, without limitation, the reasonable costs of re-testing performed to verify that any Security Issue has been remediated. Failure to remedy the risks of a Security Issue or failure within the time frame and manner specified by Buyer is deemed a material breach of this policy, the Terms and/or the Agreement.