specific terms & conditions for stc cybersecurity services

the purpose of these specific terms and conditions for stc cybersecurity services ("T&Cs") is to complement the existing terms contained in our master cloud service agreement ("MCSA").

1. definitions

1.1. all capitalized terms used but not defined herein have their meanings ascribed in the MCSA, as applicable.

"component" means each component or series of components of a solution that, which will be installed or made available to customer separately according to the installation schedule agreed to by the parties in writing including, without limitation, any third-party software.

"CPE" means the equipment (including hardware, peripherals, and related software) supplied by stc as part of the security services and managed by stc for use with such security services at the locations. CPE is never owned by the customer.

"customer" means any legal person/s (natural or corporate) that subscribes to the services either directly or through its various branches or its authorized agents/dealers.

"date of acceptance" means the date on which stc successfully completes its acceptance testing for a component. if no acceptance testing applies to a component, then the date of acceptance will be the date on which stc notifies the customer the component is ready for use or the date when customer confirms its acceptance of the component, whichever occurs first.

"final acceptance" means, for each solution, the date of acceptance of the last component to be installed or made available to the customer.

"intervention" means (i) maintenance including, without limitation, the application of updates, upgrades, patches and/or fixes, (ii) troubleshooting including, without limitation, running diagnostics and (iii) replacement, where required by stc.

"location" or "site" means the site or location at which the solution will be installed.

"penetration test" means an authorized simulated cyberattack on a customer's computer system or customer equipment, performed to evaluate the security of the system.

"security service" means all services designated by stc as security services.

"service activation" means activities necessary to activate the solution. during the course of these activities, stc may request the customer to make the necessary changes to the customer›s platform(s).

"service deactivation" means activities necessary to end the security service and disable the customer's access to the solution; this excludes the tools that the parties have agreed to remain for a certain period post the service deactivation date.

"service delivery appliance" or "SDA" means a hardware and/or software and/or virtual platform consisting of stc's scripts, configuration, and third party's products that are needed for stc to provide the security services to the customer.

"service description" refers to the document describing the security service sold to the customer by stc.

"solution" means the security services solution that stc provides to the customer pursuant to one or several order forms, as set out in the relevant service description or stc's proposal.

"target date" means, for each component, the expected date for delivery of such component to the customer as specified in the relevant order form or in the installation schedule agreed to by the parties in writing.

"third party software" refers to components whose intellectual property rights are held by third parties, including open-source software, including the software and/or solution that are provided by stc while performing a security service.

"we", "us", "our" and "stc" means stc Bahrain B.S.C. closed, incorporated under the laws of the Kingdom of Bahrain, under company registration number (71117) and having its registered address at P.O. box 21529 and its business address at building 15, road 68, block 428, Seef District, Kingdom of Bahrain.

2. application of T&Cs

2.1. these T&Cs supersede any and all statements, direct or electronic communications or promises made to the customer by any of stc's employees or agents. by concluding these T&Cs, the customer agrees that these T&Cs supersede your existing contracts or any other communications (written or verbal) with us. accordingly, the customer agrees to be bound by the following order of priority:

2.1.1 the order form

2.1.2 stc's proposal

2.1.3 these T&Cs

2.1.4 the MCSA

3. customer obligations

3.1. the customer agrees to:

3.1.1 carry out any intervention under its responsibility within the defined time limit.

3.1.2 ensure the security of its identifiers (login, password, etc.); customer is responsible for any fraudulent use of the security services that would occur from the use of its identifiers.

3.1.3 take all measures to maintain internet access to the security services. the customer is responsible for its internet access and recognize its limitations.

3.1.4 ensure prior to any Intervention by stc that all operations necessary for the protection and backup of data, programs and computer files that are under its responsibility have been performed and that all necessary measures have been taken to ensure their confidentiality and security.

3.1.5 comply with the terms and conditions of any and all licenses accompanying the relevant third-party software.

3.2. the customer will ensure, at its sole cost, that any third-party software provided by the customer and integrated to the solution is correctly licensed.

4. installation, exploitation and maintenance

4.1. as part of the solution, stc may install third party software on the customer's workstations. in this event, the customer agrees to provide stc with the original media containing the operating systems present on these workstations. the installation, operation and maintenance conditions for each service are included in the relevant service description. the customer is solely responsible for any consequence resulting from stc's intervention on these workstations, in particular any impact on any warranty or after-sales service that the customer may receive from the manufacturer/supplier of these workstations.

4.2. during the information collection stage, the customer must inform stc of applications or installed software. the customer acknowledges that stc has informed the customer that the third-party software can only be installed directly on the workstations and that it may be incompatible with certain applications or modems, or communication software already installed. stc shall not be liable in case of incompatibility between the pre-existing software and any new third party software that would cause malfunctions.

4.3. before stc installs the third-party software on the workstations, the customer agrees to backup and copy all data and software contained in the workstations. stc shall not be liable in the event that the customer has not taken all precautions relating to the backup of the data when stc installs a new third party software on a workstation.

4.4. at the time of any Intervention justified by the installation, operation or maintenance of a security service, the customer must allow stc (and any person authorized by stc) access to its premises and/or network, whether physically or virtually, where applicable. if such installation or intervention requires stc, or any person authorized by stc, to access the property of a third party, the customer is responsible for obtaining the approval of this third party.

4.5. the customer agrees to be present at the customer›s premises during stc's intervention. any period during which the customer›s premises are not accessible to stc or its agents shall not be taken into account when calculating the time required for stc to perform its obligations. in addition, stc reserves the right to charge the customer for travel and other justified expenses as well as for time spent at the hourly rate of stc or its subcontractors.

4.6. in order to maintain the quality of a security service, stc may have to perform work that could temporarily affect the proper functioning of the service. stc will make every effort to reduce any disruption that may result for the customer. in the event that such work is likely to affect the provision of the security service to the customer, stc shall notify the customer at least twenty-four (24) hours prior to the date of the operation by any means, indicating the dates, times and expected duration of the interruption of the security service. if the security service provided to the customer is the only one likely to be affected by the operation, stc will work with the customer to find a mutually agreeable time for the intervention. if, at the customer›s request, the scheduled operation takes place at a non-business hour, the additional costs are to be agreed with the customer in advance (if any). service interruptions due to scheduled maintenance operations are not considered as incidents and cannot incur the liability of stc nor be subject to penalties under stc's service level(s).

4.7. before reporting an interruption or failure of the security service to stc, the customer must first ensure that the defect is not caused by the customer's equipment or equipment for which the customer is responsible. all maintenance interventions by stc following incidents, damages or malfunctions (except in the case of scheduled maintenance operations) or originating from the internal infrastructure or from equipment not supplied by stc may lead to additional charges to be invoiced to the customer, which the parties will agree to beforehand (if any). such additional charges shall include, but not be limited to, travel and other justified expenses, time spent at the hourly rate of stc or its subcontractors, and any restoration costs.

5. delivery and acceptance

5.1. notwithstanding any term to the contrary in these T&Cs, in the event that stc or its subcontractors are unable to perform the solution, or any part of the solution, due to the customer›s non-compliance with its obligations as set forth herein, stc will not be liable for such failure and reserves the right to invoice the customer for any pre-agreed expenses, including the time spent at the hourly rate of stc or its subcontractors. furthermore, in such cases, and in particular if the customer has not complied with the requirements for which it is responsible by the target date, stc may terminate the relevant order form following ten (10) days notice, without penalty and without prejudice to any other rights at its disposal.

5.2. stc will use reasonable efforts to have each date of acceptance occur no later than the target date. stc will notify customer of the successful completion of stc's acceptance tests («service commencement notice» or «ready for service notice»). customer will be deemed to have accepted each component on the date on which stc issues a service commencement notice for that component unless customer notifies stc in writing of a material fault in the component within ten (10) days of customer's receipt of the service commencement notice. in such event, the above acceptance process will be repeated.

6. service activation and de-activation

6.1. stc will be responsible for service activation and service de-activation. stc shall be entitled to charge the time spent on activating or de-activating the service. if not otherwise agreed, such service activation or de-activation will be invoiced at either: (a) the charges agreed to in the respective order form; or (b) if charges were not agreed to, stc's current standard rates and charges (details of which stc will provide upon the customer's request).

6.2. during the service activation, the parties may identify additional preconditions needing to be met in the customer's environment prior to delivery of the relevant security service. in such case, the parties will agree on the required timeframe for the customer to comply with those conditions, and stc will inform the customer of the revised expected commencement date of the relevant security service. if stc is prevented from delivering the security service as agreed due to insufficient or incorrect information and IT set up of the customer, stc reserves the right to terminate the corresponding order form for the security service without penalty and subject to the customer's reimbursement of the agreed service activation fees to stc.

7. penetration test

7.1. stc must obtain the customer's prior written approval to perform any penetration test on the customer's systems. the parties will work together to plan tests in order to avoid and mitigate any interference in customer's overall security service delivery responsibilities.

7.2. in return and where applicable, the customer must obtain stc's prior written approval to perform any penetration test on the stc's systems. the parties will work together to plan tests in order to avoid and mitigate any interference in stc's overall security service delivery responsibilities.

8. network security and liability

8.1. the security services are designed to enhance the customer›s ability to impede unauthorized access to customer›s network and data, detect potential security breaches and identify network irregularities. however, the security services do not guarantee that all security vulnerabilities will be identified or that security incidents will be prevented. customer acknowledges that is ultimately responsible for designing and implementing a comprehensive security program that includes additional security measures beyond the scope of the security services.

8.2. stc warrants that the security services will be provided using commercially reasonable skill and care. stc disclaims all warranties, express or implied, including warranties of merchantability and fitness for a particular purpose, with respect to the ability of the security service to prevent all security breaches.

8.3. the customer acknowledges that the customer's systems, environment or data will not be entirely immunized against hacking, cyber-attacks, malicious code and/or other forms of cyber security breaches

8.4. subject to the terms set forth in clause 9 of the MCSA (our liability to you) and stc's service levels (if applicable), the parties expressly agree that stc:

8.4.1 will not be liable for any damages, direct or indirect, resulting from cyber-attacks that are not directly or indirectly caused by stc's failure of the solution that is associated with the respective security service

8.4.2 cannot ensure uninterrupted service on any network or access element providing internet connectivity and/or activities that are reliant on the performance of third-party products, connectivity services or any product. therefore, stc is not responsible for any resulting downtime or failure of delivering the security services due to such circumstances, and its liability will only be limited to the service level agreement, where applicable

8.4.3 will not be liable for any loss of the data resulting from (i) the installation, integration or maintenance of the security service, or (ii) an event external to stc. stc will not bear any costs related to the reconstruction of such data.

9. solution

9.1. unless otherwise specified in an order form, all title to and ownership of the solution and all components thereof, excluding any hardware or software provided by customer, will remain the property of stc, or its licensors.

9.2. unless otherwise specified in an order form, stc, grants to customer, for the commitment term of the applicable security services, a non-exclusive, royalty-free and non-transferable license to use the solution solely for the purpose of, and to the extent necessary for, the use of the security services.

9.3. customer undertakes that users shall not: (a) directly or indirectly attempt or allow a third party to attempt to reverse engineer, decompile, disassemble, or otherwise derive source code or other trade secrets included in the solution; or (b) add additional users to the security services in any manner designed to circumvent the obligation to pay incremental fees to either stc or any software licensor. subsections (a) and (b) in the preceding sentence are collectively and individually referred to as the «unauthorized use» of the security services.

9.4. customer will defend, indemnify and hold harmless stc and its affiliates from and against all losses arising out of or relating to any and all claims by any person or entity against stc relating to unauthorized use by a user and will pay to stc the applicable fees for any users added as described in subpart (b) above.

10. charges and invoicing

10.1. notwithstanding anything to the contrary otherwise contained in the MCSA (including an order form), if third party supplier costs to stc for the security services increase, then stc may, upon 30 days prior written notice, inform the customer that it will adjust the fees for the security services accordingly, should the customer disagree with paying such adjusted fees, stc reserves the right to suspend the impacted security services by the end of such notice period stc will invoice fees for each component from the date of acceptance of such component, except that the solution Fees will commence from the date of delivery of the solution to the customer.

11. CPE

11.1. for the avoidance of doubt, this section 11 applies to the solution.

11.2. CPE will remain the sole and exclusive property of stc or its suppliers, and no user will obtain any property rights or interest in CPE. customer will not sell, assign, sub-let, pledge or part with possession or control of CPE or any interest therein, and customer will keep CPE free from distress, liens, or claims of lien.

11.3. the parties will agree to the dates for the installation and connection of CPE, and the customer will provide all necessary assistance to enable stc to complete the installation, connection, and disconnection of CPE.

11.4. customer will not interconnect or allow the connection of CPE to any other equipment, network, or service without stc's prior written approval. any breach of this subsection 12.4 is a material breach of these T&Cs.

11.5. customer will not change, remove, or obscure any labels, plates, insignia, lettering, or other markings that stc or the manufacturer has placed on CPE. the customer will not modify or move CPE or allow anyone other than stc to modify or move CPE without stc's express written permission.

11.6. customer will maintain proper environmental conditions (e.g. air conditioning, ventilation, electrical power supply, etc.), as specified by stc or CPE manufacturers.

11.7. customer will provide a secure and safe environment for CPE with adequate access to data communications circuits and a back-up power supply, including protecting CPE from tampering and any usage outside of the provision of the applicable security service.

11.8. prior to the commencement of installation of any CPE, customer will advise stc of potential health hazards to stc personnel providing security services at the relevant Location, including any hidden power, gas or water lines, and the existence of any material constituting a health risk (e.g. asbestos).

11.9. upon termination or expiration of the relevant order form, customer will surrender possession of CPE to stc in good order, repair, and condition, reasonable wear and tear excepted.

11.10. stc will maintain CPE in good working order for the commitment term. if a lapse in the security service is caused by a failure in CPE, then stc will repair the fault following notification of the failure by the customer or detection of the failure by stc, whichever occurs first. stc may be required to dispatch a field engineer to the location to repair the CPE, and the customer will promptly provide access to the location where the CPE is installed.

11.11. stc may charge customer for visits to a Location or repairs to CPE that are required due to: (a) damage to CPE not caused by stc; (b) repairs carried out by non-stc personnel that have not been approved by stc in writing; (c) modifications to CPE that have not been approved by stc or have been carried out by personnel not approved by stc; (d) improper treatment of CPE by customer; (e) failure by customer to meet stc's or CPE›s manufacturer›s specifications on environmental conditions; or (f) user›s negligence or intentional misconduct.

11.12. customer will be liable for: (a) any loss or damage to CPE beyond reasonable wear and tear, and (b) all costs (including cost of labor and material) incurred by stc to repair or replace the lost or damaged CPE; provided that customer will not be liable for CPE loss or damage caused by, or the repair or replacement of CPE that is necessary due to, the fault of stc, stc's subcontractors, or agents. If CPE is damaged or destroyed by any user, customer will notify stc within twenty-four (24) hours of such damage.

12. termination

12.1. without prejudice to clause 13 of the MCSA, prior to the commencement of the commitment period, customer may cancel an order form upon written notice to stc and reimbursement of all amounts incurred by stc in connection with the preparation of the security service or cancellation (including, without limitation any amounts paid or payable to any third party suppliers for which stc is liable, any other unrecoverable costs and expenses incurred by stc, and a reasonable service activation fee for the applicable security service).

12.2. if customer terminates an order form for any reason during the applicable commitment period, stc may terminate the relevant security service on the customer-requested date and invoice customer for the remainder of the commitment term.

12.3. termination of an order form shall result in stc de-activating the relevant security service. in the event of such termination, customer agrees to (a) return or destroy all copies of the third-party software provided to the customer for the use of the service and (b) return to stc, if applicable, all IP addresses granted to the customer for which stc will regain full use.

13. cross-references

13.1. to the extent that any cross-references in these T&Cs do not accurately refer to provisions that address the indicated subject matter in the MCSA, the cross-references herein will be deemed to instead refer to the most closely corresponding provision(s) in the MCSA.