General Terms and Conditions

of TÜV SÜD Sec-IT GmbH (hereinafter referred to as "Sec-IT") for PCI DSS security scans

1 General

1.1 With the portal, Sec-IT provides users (hereinafter referred to as the user, client or customer) with a web-based application (hereinafter referred to as the application or portal).

1.2 Registered users can use the portal to carry out security scans (hereinafter referred to as security scans or scans).

1.3 Sec-IT performs the scan automatically using the web-based application. All activities and actions are initiated by the user and carried out using automated processes in accordance with the specifications of the user.

2 Execution and coordination

2.1 The security scans are carried out on the initiative and responsibility of the user.

2.2 All activities and actions are initiated by the user on the portal. The user shall ensure that the initiated operations are performed only for IT systems that are in possession and / or under administrative control of the user. In particular, the user may not initiate operations that target third-party systems.

2.3 If the user, contrary to the agreement set out in paragraph 2.2, initiates operations, which target third-party systems, he shall indemnify Sec-IT against any claims of third parties that may arise therefrom.

2.4 Sec-IT may engage subcontractors to provide services. For the provision of PCI services, Sec-IT shall only contract companies with valid accreditation as PCI Qualified Security Assessor [QSA] and Approved Scan Vendor [ASV] or an accredited third-party company that is in a contractual relationship with Sec-IT. The terms and conditions set forth in this contract shall apply to the same extent to subcontractors.

3 Duration and termination

3.1 The contract period is based on the arrangements set out in the order (purchase order and/or service specification).

3.2 The contract shall be extended automatically by 12 months if it is not terminated in writing by either party at least three months prior to the end of the contract period. In addition, either party may terminate the contract extraordinarily without notice for any important reason. Any notice of termination must be served in writing.

4 Obligation to cooperate

The persons responsible for the IT systems on behalf of the client must be informed by the client in advance of the PCI security scans being carried out. The client must ensure that Sec-IT or persons contracted by Sec-IT are not suspected of illegal hacking activity and that the activities carried out under the contract are not subject to prosecution.

If required, the client shall provide Sec-IT with information necessary to meet Payment Card Industry Data Security Standards. The client hereby ensures and warrants that he is aware of the requirements of the Payment Card Industry Data Security Standards.

5 Price adjustments

5.1 Sec-IT expressly reserves the right to increase prices on contract renewal. Should Sec-IT want to increase its prices for services, it shall grant the client the right of objection. If the client does not raise any objections to the price increase within 4 weeks of the written notification, the new price shall be effective from the beginning of the new contract term.

5.2 Written objections must be sent to the business address of Sec-IT. If the client objects to the price increase and the parties fail to reach an agreement on a new price by the end of the contract term, the last agreed prices shall continue to apply, and the contract will end automatically at the end of the term without the need for termination.

6 Liability

6.1 Sec-IT shall only be liable for damages, regardless of their legal basis, if Sec-IT has caused any damage as a result of an intentional or grossly negligent act or if Sec-IT has negligently breached a substantial contractual obligation („material obligation"). In the event that Sec-IT is in breach of any substantial contractual obligations, Sec-IT shall only be liable for the damage related to and typically foreseeable under the particular contract at the time of entering into the contract.

6.2 In the event that TÜV SÜD is liable under no. 6.1 above for damages caused as a result of having breached, by an act of negligence, a substantial contractual obligation, its liability shall be limited in each single case to:

> EUR 1,000,000.00 for property damage
> EUR 500,000.00 for economic loss.

6.3 Sec-IT shall not be liable for any damages caused as a result of a negligent breach of a non-substantial contractual obligation.

6.4 "Substantial contractual obligations" are those obligations that protect the customer's legal interests deemed to be substantial to the contract, which the contract, based on its content and purpose, must specifically grant to the customer; further, such contractual obligations are substantial which are deemed to be prerequisites for proper performance of a contract and upon the observance of which the customer has generally relied and may rely.

6.5 The liability exemption contained in Section 6.1-6.4 and/or the liability limits shall not apply to damage to life, person, or health; nor shall it apply for claims under a warranty or claims based on the German Product Liability Act.

6.6 The client must notify Sec-IT immediately in writing about any damage for which Sec-IT should be liable.

6.7 Sec-IT expressly points out that security scans may lead to disruption or crashes of the client's systems and cannot therefore be ruled out. Any resulting damage or consequences shall be expressly excluded from Sec-IT's liability. The client shall be obliged to perform regular backups, at least once per day, in order to ensure that in the event of data loss, data can be restored using automated procedures at a reasonable cost.

6.8 Sec-IT shall not be held liable for the accuracy, completeness, operational procedures, validity of or any changes in the compliance programme of the standard-setting body on which the assess-

ment or scanning services are based. By providing assessment services Sec-IT does not represent the client or assume liability (i) for delays or losses, (ii) for third-party claims, (iii) use and forwarding of assessment results based on compliance programmes of the standard-setting body or the results of the assessments performed on the client's behalf.

6.9 If claims for damages against Sec-IT are excluded or limited, this shall extend to any personal liability of any statutory organs, experts, miscellaneous employees, vicarious agents or any other auxiliary personnel of Sec-IT.

6.10 Notwithstanding the above provisions of Sections 6.1-6.9, the customer shall be obliged to obtain standard insurance cover for direct or indirect damage.

7 Terms of payment

7.1 The total price shall be invoiced in the case of annual contracts or fixed-price offer. The invoice shall be issued for the contracted items listed in our quote one year in advance. All other services shall be invoiced once the agreed service has been provided.

7.2 If there are delays in the provision of services due to the client's failure to comply with his obligation to cooperate or if the performance of Sec-IT is delayed due to the client's non-compliance with the obligation to cooperate, the client shall not be entitled to a refund of the full price. Sec-IT shall provide the agreed service without prejudice to the foregoing.

7.3 Any extra or additional scans that exceed the number of security scans specified in the service specification shall be invoiced separately. Sec-IT shall provide the client with a separate quote for these additional scans.

7.4 All prices are net prices i.e. exclude VAT at the applicable rate. The VAT shall be shown separately on the invoice.

7.5 Any queries regarding Sec-IT 's invoices must be submitted in writing together with the reasons for querying the invoice within 14 days of receipt of the invoice.

8 Confidentiality, usage rights, data protection

8.1 Sec-IT shall be entitled to make copies and file any documents made available to Sec-IT, which are important for the performance of the contract.

8.2 Sec-IT shall retain copyright and any other intellectual property rights in and to all components of the portal, including its layout, as well as the entire content. The client shall respect the rights of Sec-IT and in particular not alter the content by changing or removing copyright notices and/or trademarks or other information.

8.3 Sec-IT shall grant the customer a non-exclusive and non-transferable right to use the portal to carry out PCI DSS security scans. This shall expressly exclude the granting of any other industrial property rights, in particular, the use of the business name or the trademark "TÜV" and "TÜV SÜD".

8.4 The employees and experts of Sec-IT shall not, without authorisation, disclose any business and operational information they become apprised with in connection with the performance of their duties to third parties.

8.5 The non-disclosure obligation shall not apply, if Sec-IT is obliged in accordance to PCI guidelines, to provide information about the compliance status, as well as the final audit reports to the card organisations or organisations appointed by them for the final certification of the customer.

8.6 Sec-IT shall process and use personal data solely for its own purposes within the TÜV SÜD Group. Sec-IT shall only disclose data to affiliated undertakings within the meaning of Article 15 of the German Stock Corporation Act (AktG). To this end, Sec-IT will also use automated data processing systems. In order to meet the data protection requirements outlined in the Annex to Article 9 of the Federal Data Protection Act (BDSG), Sec-IT has taken technical and organisational measures to ensure the security of its data and data processing operations. The employees engaged in data processing are bound by the BDSG and are expected to observe all data protection regulations strictly.

9 Place of jurisdiction, applicable law

9.1 The place of jurisdiction for the assertion of claims shall be Munich.

9.2 The contractual relationship and all legal relations arising from it shall be exclusively governed by, and construed in accordance with the laws of the Federal Republic of Germany without regard to its provisions of the Conflict of Laws and the UN Convention on the Sale of Goods (CISG) which shall be expressly excluded.

10 Access data and miscellaneous

10.1 The client shall be obliged to keep all access data to the portal strictly confidential and shall not disclose it to third parties. The customer shall be held responsible for any actions carried out on the portal using his access data.

10.2 Where Sec-IT contains links to third-party websites, Sec-IT shall not accept any responsibility or liability for the content of such third-party websites. Sec-IT expressly distances itself from the content of all third-party websites, as it is not possible to control third-party websites on an ongoing basis. The client shall therefore use or follow these links to third-party websites at his own risk.