AGREEMENT SECURITY TEST

AGREEMENT SECURITY TEST BIT B.V. - VERSION 2019-8-20

1. Article 1: LIMITATION
   - 1.1 Infrastructure and/or information systems of BIT that are not part of the security test and infrastructure and/or information systems of BIT's customers other than Client, will not be used as a stepping stone for accessing the systems that are part of the security test.
   - 1.2 Auditor will make all reasonable efforts to refrain from any activities that will jeopardize the confidentiality, integrity or availability of information systems from BIT or BIT's customers other than Client (i.e. DDoS attacks). Whilst Auditor will conduct all security test activities in line with accepted best practice, the tools and techniques used may cause disruption to BIT's information systems and/or possible loss of or corruption to data and BIT agrees to take such backups and provide such redundant systems as are prudent in the circumstances. Auditor will notify BIT in the event where activity would lead to loss of service or data where this is known to Auditor.
   - 1.3 In case the security test activities jeopardize the confidentiality, integrity or availability of information systems from BIT or BIT's customers other than Client, BIT can request Auditor and/or Client to halt the security test immediately.
   - 1.4 BIT may take actions, without prior consultation with Auditor and/or Client, that limit or halt the security test in case the confidentiality, integrity or availability of information systems from BIT or BIT's customers other than Client are in jeopardy.

2. Article 2: PERMISSION AND INDEMNIFICATION
   - 2.1 Because breaking into computer systems without permission is a crime according to Dutch law, BIT gives explicit permission to Auditor to perform the agreed activities for the Client.
   - 2.2 Because performing the security test activities for the Client might go against BIT's Acceptable Use Policy, BIT declares this Acceptable Use Policy and its Abuse Policy inapplicable for the security test activities during the given time frame as described in article 16.
   - 2.3 The Service Level Agreement(s) BIT offers to Client will not be applicable during the security test and any aftermath of the security test.
   - 2.4 BIT indemnifies Auditor against claims of BIT, BIT's customers and third parties that are associated to BIT and/or BIT's customers – for both direct and indirect (subsequent) damages – which are caused by or related to the security test activities. This article does not apply in case of gross negligence, malicious intent or non-compliance with any provisions of this agreement by Auditor.

3. Article 3: DATA BREACH
   - 3.1 If during the security test activities any data from BIT, BIT's customers or any third party becomes accessible to Auditor, Auditor will limit its access to this data as far as it is necessary for the security test activities.
   - 3.2 Auditor will delete any copies of the data described in article 12 immediately after completing the security test activities.

4. Article 4: INFORMATION SHARING
   - 4.1 Auditor will share with BIT the vulnerabilities on BIT's infrastructure and/or BIT's information systems and/or information systems from BIT's customers, that were found during the security test activities.
   - 4.2 For the type of security tests/attacks that cannot be executed because of limitations BIT imposed, BIT can, on request, inform Auditor/Client on pre-emptive/mitigating measures that BIT has in place to prevent these type of attacks in real life (i.e. DDoS attacks).

5. Article 5: CONTACT
   - 5.1 Client will inform BIT on the systems and/or applications that are part of the security test and the time frame in which the security test activities will take place.
   - 5.2 Auditor will inform BIT on the IP addresses he will use to perform the security test activities.
   - 5.3 Auditor and Client will inform BIT on names, telephone numbers and email addresses of direct contact persons or departments within their organisation regarding the security test activities.
   - 5.4 BIT's customer service email address is info@bit.nl. Use cert@bit.nl with PGP KeyID 9DCA4A97A80E77B1 for any information that needs to stay secretive. For emergencies BIT can only be contacted by phone, 24x7 on +31 318 648 688.

6. Article 6: CONFIDENTIALITY
   - 6.1 All information and data that gets exchanged between Auditor, Client and BIT or which becomes known, including but not limited to software, preparation materials, documentation, knowledge or company secrets of Auditor, Client and BIT, will be treated as confidential by all parties. The receiving party will use this information only for the intended purpose and not disclose this information to third parties, other than after written permission or in case of a legal

obligation. BIT may share information regarding vulnerabilities found on information systems from BIT's customers with the customer in question.