1 Limitations

1.1 Infrastructure and/or information systems of BIT that are not part of the security test, as well as infrastructure and/or information systems of other BIT clients, shall not be used as a stepping stone to access systems included in the security test.

1.2 The Auditor shall make all reasonable efforts to refrain from activities that jeopardise the confidentiality, integrity, or availability of BIT's or other BIT clients' information systems (e.g., DDoS attacks). While the Auditor will perform all security test activities to the best of their ability, the tools and techniques used may disrupt BIT's information systems and/or result in potential data loss or corruption. BIT agrees to provide necessary backups and redundant systems as required under the circumstances. The Auditor shall notify BIT if an activity causes service disruption or data loss, provided the Auditor is aware of such an incident.

1.3 If the security test activities compromise the confidentiality, integrity, or availability of BIT's or other clients' information systems, BIT may request the Auditor and/or Client to immediately halt the security test.

1.4 BIT may, without prior consultation with the Auditor and/or Client, take actions to impede or terminate the security test if the confidentiality, integrity, or availability of BIT's or other clients' information systems is compromised.

2 Consent and Indemnification

2.1 As unauthorised access to computer systems constitutes a criminal offence under Dutch law, BIT explicitly grants the Auditor permission to perform the agreed activities for the Client.

2.2 Since the security test activities for the Client may contravene BIT's Acceptable Use Policy, BIT declares that the Acceptable Use Policy and the Abuse Policy do not apply to the security test activities during the timeframe specified in Article 16.

2.3 The Service Level Agreement(s) offered by BIT to the Client shall not apply during or as a result of the security test.

2.4 BIT indemnifies the Auditor against claims from BIT, BIT clients, and third parties associated with BIT and/or its clients—including direct or indirect (consequential) damages—arising from or related to the security test or its activities. This clause does not apply in cases of gross negligence, wilful misconduct, or non-compliance with this agreement by the Auditor.

3 Data Breach

3.1 If the security test activities result in access to data belonging to BIT, BIT clients, or a third party, the Auditor shall limit such access to the extent possible within the scope of the test.

3.2 The Auditor shall delete all copies of the data described in Article 3.1 immediately upon completion of the security test activities.

4 Information Sharing

4.1 The Auditor shall disclose to BIT any vulnerabilities found in BIT's infrastructure, BIT's information systems, or BIT clients' information systems during the security test.

4.2 For security test/attack types that cannot be executed due to restrictions imposed by BIT, BIT may, upon request, inform the Auditor/Client of preventive/restrictive measures implemented to mitigate such attacks (e.g., DDoS attacks).

5 Contact

5.1 The Client shall inform BIT of the systems and/or applications included in the security test and the timeframe for its execution.

5.2 The Auditor shall notify BIT of the IP addresses used to conduct the security test activities.

5.3 The Auditor and Client shall provide BIT with the names, phone numbers, and email addresses of direct contacts or departments responsible for the security test.

5.4 BIT's customer service email is info@bit.nl. Use cert@bit.nl with PGP KeyID 9DCA4A97A80E77B1 for confidential communications. For emergencies, BIT is available 24/7 by phone at +31 318 648 688.

6 Confidentiality

6.1 All information exchanged between the Auditor, Client, and BIT, or otherwise disclosed—including but not limited to software, preparatory materials, documentation, knowledge, or trade secrets—shall be treated as confidential by all parties. The receiving party shall use such information solely for its intended purpose and not disclose it to third parties, except with written consent or under legal obligation. BIT may share information about vulnerabilities found on BIT clients' information systems with the affected client.