Terms and Conditions for AppCheck Vulnerability Scanning Services (AppCheck Service)

1. These terms and conditions are to be viewed in conjunction with the General Terms and Conditions for IT Security.
2. The AppCheck Service is provided as either a managed external service via the AppCheck cloud-based portal, or as a managed internal service provided via a virtual appliance (the Internal Hub). The type of AppCheck Service and the term of the service provided is specified in the Order.
3. You must provide written acceptance of the AppCheck Acceptable Use Policy found at https://scanner.appcheck-ng.com/assets/acceptable_use_policy.pdf by completing the AppCheck Vulnerability Scanning Service Permission Form prior to the AppCheck Service being provided.
4. Upon acceptance of the AppCheck Acceptable Use Policy and upon receipt of a completed AppCheck Vulnerability Scanning Service Permission Form, signed by your authorised representative, we will provide the AppCheck Service on pre-arranged dates to be agreed between both parties.
5. Where it is identified, as a result of the AppCheck Service, that remediation works are required, the cost of any such remediation works is not included within the Agreement.
6. You agree to:
   - 6.1. Ensure that the AppCheck Vulnerability Scanning Service Permission Form is completed accurately and by your authorised representative.
   - 6.2. Be responsible for obtaining and maintaining all licences, permissions and consents from third parties prior to the AppCheck Service being provided.
   - 6.3. Be wholly responsible for the security of your proprietary and Confidential Information and Data, including the personal data of individuals held on the System.
   - 6.4. Warrant that the System is sufficiently robust to support and facilitate the provision of the AppCheck Service.
   - 6.5. Maintain up to date back-up copies of the configuration for software and hardware and the programs and Data necessary to restore the System to its original state on completion of the provision of the AppCheck Service and ensure that such back-up copies are kept up to date and in order, and available for use at all times.
   - 6.6. Agree that you will only use the results of the AppCheck Service provided for your own internal business purposes and will not disclose the results to any third party without our prior written consent.
   - 6.7. Where the AppCheck Internal Hub Service is provided, you agree that you will:
     - 6.7.1. not copy nor interfere with the Internal Hub and will not make the Internal Hub available to any third party, or attempt to duplicate the Internal Hub to enable it to be run on more systems than permitted by its licence.
     - 6.7.2. ensure that the Internal Hub is, at all times, secure and is only used by us as part of the managed service in accordance with these terms
     - 6.7.3. not make, or attempt to make, any alterations or modifications to the Internal Hub, nor disassemble, decompile, reverse engineer or create derivative works based on any part of the Internal Hub.
   - 6.8. Ensure that your instructions for the usage and your usage of the AppCheck Service are in accordance with any legislation which is applicable to the performance of scans or any of the other Services performed under this agreement, including the Computer Misuse Act 1990, the Investigatory Powers Act 2016 and the Data Protection Act 2018 incorporating the UK GDPR (Applicable Law).
   - 6.9. Where the AppCheck Service is used on a System containing personal data, ensure there is a lawful basis for processing and provide each data subject, whose personal data is or may be disclosed, with the fair processing information as required by Applicable Law and immediately notify us if you receive a request from a data subject to exercise his/her rights under Applicable Law.
   - 6.10. Acknowledge and accept that:
     - 6.10.1. the methods used by the AppCheck Service may include methods and techniques of a type usually deployed by hackers or which are otherwise designed to cause systems to function in a manner other than that which is intended or to gain unauthorised access to systems, networks and the data stored within them; and
     - 6.10.2. the AppCheck Service may expose vulnerabilities and/or disruption to service and, particularly where the using services, such as exploitive scans, which carry a substantial risk of loss of service, hardware failure and loss or corruption of data
   - 6.11. Indemnify us from and against all costs, claims, damages, liabilities, loss and demands relating to or arising from or in connection with any criminal or civil legal action brought as a result of the use of the AppCheck Service or our performance of any of the Services (provided that we perform the Services in accordance with these terms), including as a result of or in connection with:
     - 6.11.1. any breach of Applicable Law which you or we are alleged to have committed as result of using the AppCheck Service
     - 6.11.2. where inaccurate information is provided to us causing a third party system or network to be scanned where we are not authorised to do so, including any consequences arising out of action taken by a third party hosting provider where you fail to obtain the necessary approval
     - 6.11.3. the AppCheck Service causing any loss or damage to your System and any claim that is made by a third party
     - 6.11.4. any unauthorised third party gaining access to the AppCheck Service using your access credentials.