ACCEPTABLE USE POLICY

About this Acceptable Use Policy

AppCheck[NG] is a web application and infrastructure vulnerability scanner, deployed as a single SaaS scanning system or as part of a distributed scanning network.

We are AppCheck Ltd, a company registered in England and Wales with registered number 06888174 and VAT number GB203666327. Our registered office is Unit 19, Pavilion Business Park, Royds Hall Road, Leeds, LS12 6AJ.

We offer AppCheck[NG] on a paid subscription basis, both directly and through our carefully selected partners. Access to AppCheck[NG] is only available to our subscribers' authorised users (or to users who are using AppCheck[NG] on a trial basis). You must therefore only attempt to access AppCheck[NG] if you are an employee, consultant or agent of one of our subscribers or an organisation which is trialling AppCheck[NG] and the entity has given you permission to access AppCheck[NG] on its behalf.

We are keen to get you started with AppCheck[NG] as soon as possible, but before we do there are a few important things you need to know about making proper and effective use of the service.

Please read this document carefully and let us know if you have any questions before you get started. By ticking the acceptance box on our login screen and proceeding with your log in you confirm you will comply with this policy.

1. BEFORE STARTING A SCAN

1.1 When you log in to AppCheck[NG], you will have the ability to carry out vulnerability scans on your chosen URLs and IPs to identify and confirm vulnerabilities through safe exploitation. Once the scan is complete, AppCheck[NG] will generate a report detailing any identified vulnerabilities.

1.2 It is essential that you carefully check the details of all applications and IPs that you want to scan, to ensure both that your organisation has the right to authorise us to undertake the scan and that you have the necessary internal authority and/or approval to undertake that scan.

1.3 Where the system is provided by a third party hosting provider, we recommend that you provide the hosting provider with advance notice of the scan and/or ask the hosting provider to white list our IPs.

1.4 Before you start a scan, it is essential that you read the following warnings carefully. By proceeding with the scan, you confirm that you acknowledge and agree to the following:

1.4.1 The methods we use 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.

1.4.2 The scanning performed by AppCheck may expose vulnerabilities and/or cause disruption to, malfunction of or other unexpected functioning of the systems you are scanning and carries a risk of loss of service, hardware failure and loss, compromise or corruption of data.

1.5 Before starting a scan, we strongly advise you to:

1.5.1 Complete a full backup of all data which is contained in or available through any devices connected to any systems to be scanned, and to ensure that the backup is stored remotely from the scanned system.

1.5.2 Ensure that the scan is being performed at a time when any adverse impact on the systems being scanned is unlikely to cause a material impact to its business.

1.5.3 Ensure that there are sufficient qualified and knowledgeable representatives available to respond promptly to any vulnerability identified and to deal with any adverse impact that the scan may cause on the systems.

2. MAKING PROPER USE OF APPCHECK[NG]

2.1 There is no limit on the total number of scans you can carry out, but there is a restriction on the number of scans which can be carried out concurrently, and scans may only be carried out within the number of applications and IPs that the subscriber has licensed or the applications and IPs which form part of the trial. Please check with your organisation for more information as to the scope of its subscription or trial.

2.2 You must only ask us to scan applications and IPs which are on a system or network which your organisation uses exclusively in connection with its own business requirements and which it has the right to scan.

2.3 You must use AppCheck[NG] in accordance with this Acceptable Use Policy, in good faith and in the manner in which is intended.

2.4 You must not use AppCheck[NG] in a manner that breaches any applicable local, national or international law or regulation, which may damage our reputation, that of AppCheck[NG], or that of any client or user and/or which is unlawful or fraudulent, or has any unlawful or fraudulent purpose or effect.

3. WHAT TO DO ONCE THE SCAN IS COMPLETE

3.1 The scan is designed to identify and confirm vulnerabilities and report to you on any vulnerabilities. However, the scan will not (and is not intended to) fix, remedy, prevent or eliminate any vulnerabilities or other issues.

3.2 If vulnerabilities are identified, you will receive a report containing recommended fix steps and links to solutions. If the report does identify any issues, you should deal with those vulnerabilities in accordance with your organisation's own internal policies and procedures.

4. IMPORTANT INFORMATION FOR DIRECT SUBSCRIBERS

If you are accessing AppCheck[NG] on behalf of a direct subscriber (a subscriber which took out its subscription directly with us and not through a partner), you should read the following information carefully:

4.1 This Acceptable Use Policy supplements and does not replace the subscriber's existing subscriber agreement, and nothing in this Acceptable Use Policy replaces or overrides any provision of the subscription agreement.

4.2 This Acceptable Use Policy is intended only to deal with the proper use of AppCheck^{NG}. It does not create any direct contractual entitlement for you to receive the services, nor does it provide you with any direct remedies if you experience a problem with the service. If you experience any issues arising out of your use of AppCheck^{NG} you should ask the subscriber to raise these with us directly.

4.3 All subscribers who have signed up or renewed their subscription since April 2019 will have electronically signed a copy of our subscription agreement which sets out the commercial and legal terms which apply to their subscription. These subscribers should refer to their subscription agreement for more information.

4.4 If you are accessing AppCheck^{NG} on behalf of a subscriber who signed up before April 2019, use of AppCheck^{NG} will continue to be governed by our legacy terms for the remainder of the subscription term (these can be accessed at https://scanner.appcheck-ng.com/assets/terms.pdf). By logging into AppCheck^{NG} you agree to those terms and conditions on behalf of the subscriber (and acknowledge that you have authority to do so).

5. IMPORTANT INFORMATION FOR PARTNER SUBSCRIBERS

If you are accessing AppCheck^{NG} on behalf of a partner subscriber (a subscriber which took out its subscription through one of our partners, rather than directly with us), you should read the following information carefully:

5.1 This Acceptable Use Policy supplements and does not replace the subscriber's existing agreement with the partner. Nothing in this Acceptable Use Policy replaces any provision of the subscriber's agreement with the partner.

5.2 This Acceptable Use Policy does not establish a direct contractual relationship between us and you or between us and the subscriber, nor does it give you or the subscriber any direct rights or remedies against us. If you experience any issues arising out of your use of AppCheck^{NG} you should ask the subscriber to raise these with the partner directly.

5.3 Although the subscriber's obligations are primarily set out in its agreement with the partner, to protect ourselves and AppCheck^{NG} we require the subscriber to provide certain undertakings to us. The following are legally binding commitments and, by logging into AppCheck^{NG}, you agree to these terms and conditions on behalf of the subscriber (and acknowledge that you have authority to do so):

5.3.1 The subscriber must take responsibility for its users and their compliance with this Acceptable Use Policy, and the subscriber will be directly responsible to us for any breach by a user of this Acceptable Use Policy.

5.3.2 The performance of the scan is governed by various laws, including the Computer Misuse Act 1990, the Investigatory Powers Act 2016 and the UK GDPR. By running a scan you expressly authorise us (on the subscriber's behalf) to access (or attempt to access) the subscriber's systems (and any programs or data held on those systems) and to perform any actions, operations or exploits which we consider reasonably necessary or desirable to enable us to identify and confirm vulnerabilities present on those systems.

5.3.3 To ensure compliance with data protection legislation, you must ensure that the subscriber has appropriate data processing terms in place with the partner prior to commencing any scan, and these terms must comply with the requirements of the UK GDPR and permit the partner to appoint us at its sub-processor.

5.3.4 The subscriber agrees to indemnify us against:

(a) Any breach of applicable law which we or the subscriber are alleged to have committed.

(b) Your use of AppCheck^{NG} to scan a system or network where you are not authorised to do so, including any consequences arising out of action taken by a third party hosting provider.

(c) Any loss or damage caused as a result of us performing the scan on the requested system.

(d) All claims, demands, penalties, fines, actions, costs, expenses, losses and damages we suffer or incur or which are awarded against us arising from or in connection with any failure by the subscriber to comply with paragraph 5.3.2 or 5.3.3.

(e) Where the subscriber obtains a third party service through the partner which is provided to the partner by us, any failure by the subscriber to use that third party service in good faith and in the manner in which is intended and in accordance with any terms or other requirements or directions imposed by the provider of that service, or any steps taken by the subscriber which are intended or likely to cause the provider of the third party service to terminate its relationship with us or to pursue any claim against us.

5.3.5 All rights, title and interest (including intellectual property rights) in AppCheck^{NG} and the report that we generate will (as between us and the subscriber) belong to us, and nothing in these terms will operate to transfer any of those rights to the subscriber. The subscriber is entitled to use the report for the purposes of reviewing its findings and acting on them to address any vulnerabilities identified.

6. IMPORTANT INFORMATION IF YOU ARE USING APPCHECK^{NG} AS PART OF A TRIAL

If you are an organisation signing up for a trial of AppCheck^{NG}, you must read the following information carefully and you acknowledge that by signing up for a trial, you are accepting the terms set out below. If you are accessing AppCheck^{NG} on behalf of an organisation which is currently trialling AppCheck^{NG}, you should read the following information carefully and ensure that you understand and comply with any relevant provisions:

6.1 During the term of the trial, AppCheck^{NG} is provided on an "as-is" and "as-available" basis without any form of warranty, guarantee or other assurance or commitment, and AppCheck^{NG} excludes any liability that it may otherwise have to the organisation trialling AppCheck^{NG} to the maximum extent permitted by law.

6.2 AppCheck reserves the right to suspend, terminate or vary the terms of a trial at any time for any reason.

6.3 The performance of the scan is governed by various laws, including the Computer Misuse Act 1990, the Investigatory Powers Act 2016 and the UK GDPR. By running a scan you expressly authorise us (on your organisation's behalf) to access (or attempt to access) the relevant systems (and any programs or data held on those systems) and to perform any actions, operations or exploits which we consider reasonably necessary or desirable to enable us to identify and confirm vulnerabilities present on those systems.

6.4 The organisation trialling AppCheck^{NG} agrees to indemnify us against:

6.4.1 Any breach of applicable law which we or the organisation are alleged to have committed.

6.4.2 Its use of AppCheck^{NG} to scan a system or network where the organisation is not authorised to do so, including any consequences arising out of action taken by a third party hosting provider.

6.4.3 Any loss or damage caused as a result of us performing the scan on the requested system.

6.4.4 All claims, demands, penalties, fines, actions, costs, expenses, losses and damages we suffer or incur or which are awarded against us arising from or in connection with any failure by the subscriber to comply with paragraph 6.3.

6.5 All rights, title and interest (including intellectual property rights) in AppCheck^{NG} and the report that we generate will (as between us and the organisation trialling AppCheck^{NG}) belong to us, and nothing in these terms will operate to transfer any of those rights to that organisation. The organisation is entitled to use the report for the purposes of reviewing its findings and acting on them to address any vulnerabilities identified.

6.6 Where AppCheck^{NG} is used to scan a system containing personal data, it is possible that the scanning engine may gain access to personal data stored on that system and that this personal data may be recorded in the logs of the scan. This may constitute "processing" for the purposes of data protection legislation. Should any processing occur:

6.6.1 the types of personal data processed and the categories of data subject to which that personal data relates will depend on the nature of the data accessed and could include any type of personal data and any category of data subject;

6.6.2 we will process that personal data only in accordance with these terms and your organisation's documented instructions (unless otherwise required by law in which case we will, where permitted, inform your organisation of that legal requirement before processing);

6.6.3 we will implement appropriate technical and organisational measures in respect of our processing of that personal data to ensure a level of security appropriate to the risk (in compliance with article 32 of the UK GDPR);

6.6.4 we will ensure that any persons authorised to process the personal data on your organisation's behalf are subject to a duty of confidence in respect of that processing;

6.6.5 other than as permitted by Chapter V of the UK GDPR, we will not transfer or allow the transfer of that personal data outside the United Kingdom without your organisation's written consent;

6.6.6 if we become aware of any personal data breach occurring in connection with our own processing of the personal data, we will notify your organisation without undue delay and, where applicable, assist you to comply with your obligation to inform a regulatory authority and/or affected data subjects of the personal data breach;

6.6.7 we will provide any assistance your organisation may reasonably request in your performance of your own obligations under the UK GDPR as required by Articles 28(3)(e) and (f) at your organisation's reasonable expense.

6.6.8 your organisation authorises us to engage sub-processors from time to time provided that we will notify you of any intended changes concerning the addition or replacement of sub-processors and will impose upon any sub-processor (and ensure any sub-processor's compliance with) these terms as if the processing being carried out by the sub-processor was being carried out by us (and we will be liable for the acts and omissions of its sub-processors as if they were our own acts and omissions);

6.6.9 upon your written request, we will provide details in writing of the data processing activities carried out on your organisation's behalf;

6.6.10 upon reasonable notice we will allow your organisation (or its appointed auditor) to audit our compliance with the terms set out in this paragraph 6.6, subject to any reasonable requirements or restrictions that we may impose to safeguard the personal data we hold on behalf of other organisations and/or avoid unreasonable disruption to our business;

6.6.11 we will process personal data on your organisation's behalf only during the period of the trial (and after the expiry of the trial to the extent required to perform any post termination obligations); and

6.6.12 on the expiry of the trial, we will either delete or return all personal data processed on your organisation's behalf, and delete any copies, except

(a) if your organisation signs up for a subscription, in which case we will process the personal data in accordance with our subscription terms; or

(b) to the extent retention is required by law or for record-keeping.