SEQRITE PRODUCT SPECIFIC TERMS

IMPORTANT – READ CAREFULLY: These Seqrite Product Specific Terms consists of additional terms and conditions for the Software or Cloud Offerings set forth herein and licensed under the Seqrite End-User License Agreement (**"Agreement"**) between You and Quick Heal Technologies Limited (**"Seqrite"**). Please note that there may be certain terms in these Seqrite Product Specific Terms that do not apply to You. Only those terms related to the specific Software or Cloud Offerings licensed to You under the Agreement are applicable to You. Except as set forth in these Seqrite Product Specific Terms, capitalized terms shall have the meaning set forth in the Agreement. To the extent that there is a conflict between the Agreement and Seqrite Product Specific Terms, these Seqrite Product Specific Terms shall take precedence. Further, these Seqrite Product Specific Terms may be changed from time to time and such changes shall be effective immediately upon posting of such changes on the website of Seqrite.

SEQRITE PRODUCT SPECIFIC TERMS:

1. **Seqrite Unified Threat Management (UTM) Software:**
In the event You have purchased License to Seqrite UTM Software, the terms and conditions of Hardware Warranty and Return Material Authorization (RMA) Policy for Seqrite UTM Hardware shall be applicable and binding upon You, apart from this Agreement. The said Policy for Seqrite UTM Hardware Warranty and RMA can be accessed at the below link, and is subject to revisions from time to time.

https://www.seqrite.com/documents/en/misc/Seqrite_UTM_Return_Material_Authorization_Policy.pdf

2. **Seqrite Endpoint Protection and Seqrite Endpoint Protection Cloud (*Formerly known as Seqrite End Point Security and Seqrite Cloud EPS*):**

2.1 Nature of Product: Seqrite Endpoint Protection (EPP) is a comprehensive endpoint security software solution designed to protect workstations, laptops, servers from a wide range of cyber threats. It offers features for prevention, detection, response, and threat hunting, catering to both on-premises and cloud environments as Seqrite Endpoint Protection and Seqrite Endpoint Protection on cloud.

2.2 Functionality of Product and Consequences:

2.2.1 Functionality:

2.2.1.1 Protection: EPP provides protection against malware, ransomware, phishing attacks, intrusion attempts, vulnerabilities, and data loss.

2.2.1.2 Management and Control: It offers centralized management of security policies, patches, devices, and applications.

2.2.1.3 Visibility and Reporting: EPP provides real-time insights into endpoint activity, vulnerabilities, and threats.

2.2.1.4 Scalability and Flexibility: The solution can be deployed on-premises or in the cloud, adapting to various business needs.

2.2.2. Consequences: Users are responsible for maintaining system hygiene, following security best practices, and keeping software updated.

2.2.3. Usage of information sets by Seqrite:

2.2.3.1 Collected Information: EPP may collect information about endpoints, applications, vulnerabilities, threats, and user activity.

2.2.3.2 Purpose of Use: This information is used to provide security services, detect threats, analyze trends, and improve product functionality.

2.2.3.3 Data Security: Seqrite implements measures to protect collected information in accordance with the Agreement.

3. Seqrite Data Privacy (*Formerly known as Seqrite HawkkScan*):

3.1 Nature of Product: Seqrite Data Privacy is a cloud-hosted software (i.e. SaaS) offering. Enterprises use Seqrite Data Privacy to meet their data privacy and data compliance requirements. Towards this objective, You can connect Your data sources, whether on-premises or on the cloud, to Seqrite Data Privacy.

3.2 Functionality of Product and Consequences: Deep discovery scans and incremental discovery scans run by Seqrite Data Privacy on Your connected data sources may result in personal data or personally identifiable information and their potential locations being discovered per the data classifiers configured by You in Seqrite Data Privacy. These personal data or personally identifiable information sets may belong to Your end-customers or employees.

3.3 Usage of information sets by Seqrite: Seqrite Data Privacy being a SaaS offering, securely stores these information sets per cloud tenant. There may possibly be cross-border transfer of this information depending upon the geo-location of Your data sources, which shall be carried out by Seqrite in accordance with Seqrite's Privacy Policy and applicable data privacy laws. Seqrite Data Privacy does not in any way share these information sets anonymously or otherwise in any manner whatsoever, across its cloud tenants or other End-User. Further, Seqrite does not process, store, or transmit this information in any way out of a cloud tenant. All activities in a cloud tenant are fully restricted to activities performed by You (i.e. tenant owner in this case) in the course of using the Seqrite Data Privacy SaaS software.

4. Seqrite XDR (*Formerly known as Seqrite HawkkHunt XDR*):

4.1 Nature of Product: Seqrite XDR is a cloud-hosted software (i.e. SaaS) offering. Seqrite XDR is an advanced detection and incident response solution that analyses alerts collected from various sources and correlates this data to discover advanced persistent threats. In order to provide you with its relevant technical functionalities by discovering potential threats and sensitive data exfiltration attempts, Seqrite XDR processes Your email content and files or documents. You, therefore, consent to and authorize Seqrite for such processing of Your email content and files or documents for the limited purpose of making available to You with the prescribed technical functionalities. For the avoidance of doubt, it is expressly clarified and agreed that Seqrite does not store or retain Your unprocessed email content and files or documents. In the event You are required to submit Your email content and files or documents to Seqrite while accessing and using Seqrite XDR, You hereby agree that You have ensured that the files or data submitted by You do not contain any personal or sensitive data. You, therefore, acknowledge and agree that: (i) it is not the responsibility of Seqrite to verify the contents of Your submission while You access and use Seqrite XDR; (ii) Seqrite may share Your specimen submission or documentation with the information technology security fraternity and data associations; and (iii) You will not submit any personally identifiable or other sensitive information to Seqrite in any form whatsoever while submitting files and data on Seqrite XDR.

4.2 Functionality of Product and Consequences: Seqrite XDR discovers threats using custom rule builder, performs threat hunting on historical events and alerts data from the enterprise, utilizes highly customizable connectors and playbooks to extend the data enrichment and response functionalities of the product, performs incident and SLA management for the security operations center. During the collection of data from various sources, there can be certain personally identifiable information that may be collected for the tenant based on the kind of data that is sourced that can belong to Your end customer or employees.

4.3 Usage of information sets by Seqrite: Seqrite XDR being a SaaS offering, securely stores these information sets per cloud tenant. There may possibly be cross-border transfer of this information depending upon the geo-location of Your data sources, which shall be carried out by Seqrite in accordance with Seqrite's Privacy Policy and applicable data privacy laws.

Seqrite XDR does not in any way share these information sets anonymously or otherwise in any manner whatsoever, across its cloud tenants or other End-User. Further, Seqrite does not process, store, or transmit this information in any way out of a cloud tenant. All activities in a cloud tenant are fully restricted to activities performed by You (i.e. tenant owner in this case) in the course of using the Seqrite XDR. Your data shall be retained by Seqrite XDR for so long as Seqrite deems it necessary to perform the functionalities pertaining to your use of Seqrite XDR. However, it is clarified that Seqrite reserves the right to modify the data retention practices for Seqrite XDR at any time, upon prior notification through release notes.

4.4 Network Monitoring: Each network device monitored by Seqrite XDR will be treated as a separate, unique endpoint for Seqrite XDR and the limit of 1.8 GB of data per month will be applicable for each network device.

4.5 E-mail Monitoring: Each email domain monitored by Seqrite XDR will be treated as a separate, unique endpoint for Seqrite XDR and the limit of 1.8 GB of data per month will be applicable for each domain.

4.6 Cloud Monitoring: Each Cloud Service Account that is connected to by Seqrite XDR for purposes of data analysis and correlation will be treated as a unique endpoint for Seqrite XDR and the limit of 1.8 GB of data per month will be applicable for each such Account.

5. Seqrite MDR (*Formerly known as Seqrite HawkkWatch – Managed Detection and Response (MDR) Service*):

5.1 Functionality: Seqrite MDR is an optional, cloud based add-on to Seqrite XDR, where Seqrite MDR Response team helps the customer's security team in responding to advanced cyber-attacks. The key features of Seqrite MDR are Incident Response 24/7, Root Cause Analysis, Threat Intelligence & Threat Hunting and Generating monthly reports on threat activity & response preparedness and performance; suggests training & improvement.

5.2 Remote Access – Customer Consent; Representations and Warranties: Subject to Your express consent and authorization, Seqrite may acquire remote access to the endpoints of Your device, solely for the purposes of restoring Your device while performing MDR Service. You acknowledge, understand and agree that unauthorized access to computer systems or devices may not be permitted by applicable laws. You, therefore, represent and warrant to Seqrite that: (i) You have obtained all applicable consents and authority for Seqrite to perform the MDR Service; (ii) Such remote access by Seqrite does not violate any applicable law or any obligation You owe to a third party; (iii) You are the owner or licensee of any device upon which Seqrite performs the MDR Service; (iv) You are authorized to instruct Seqrite to perform MDR Service on Your device; and (v) You further assume all risk and liability in this regard and Seqrite shall have no liability in this regard whatsoever.

5.3 Service Level Terms: The Service Level Terms for Seqrite MDR are as follows:

Minor Assistance Requests	For low priority Incidents	24 hours from creation/updation of the Incident
Critical Assistance Requests	For Critical Incidents raised by XDR or customer SOC	Engineer shall be made available within 30 mins of Request

Number of Standard Assistance requests that can be serviced in a calendar month	Beyond this, it will be on a best effort basis without any standard penalty	20
Number of Minor Assistance Requests that can be serviced in a calendar month	Beyond this number, it will be on a best effort basis without any standard penalty considerations	100
Number of Critical Assistance Requests that can be serviced in a calendar month	Beyond this number, it will be on a best effort basis without any standard penalty considerations	4

6. Seqrite Managed Security Service Portal (MSSP):

Seqrite MSSP is a SaaS platform enabling seamless deployment and management of multi-tenant or multi-customer Seqrite Centralized Security Management sites. As a part of the sign-up and on-boarding process, Seqrite MSSP requires You to submit certain types of data or information. By submitting the files or data to Seqrite while accessing and using Seqrite MSSP, You hereby agree that You have ensured that the files or data submitted by You do not contain any personal or sensitive data. You, therefore, acknowledge and agree that: (i) it is not the responsibility of Seqrite to verify the contents of Your submission while You access and use Seqrite MSSP; (ii) Seqrite may share Your specimen submission or documentation with the information technology security fraternity and data associations; and (iii) You will not submit any personally identifiable or other sensitive information to Seqrite in any form whatsoever while submitting files and data on Seqrite MSSP.

7. Seqrite Enterprise Mobility Management (*Formerly known as Seqrite mSuite*):

Seqrite Enterprise Mobility Management is a SaaS platform enabling seamless deployment and management of multi- tenant or multi-customer Seqrite sites. As a part of the sign-up and on-boarding process, Seqrite Enterprise Mobility Management requires You to submit certain types of data or information. By submitting the files or data to Seqrite while accessing and using Seqrite Enterprise Mobility Management, You hereby agree that You have ensured that the files or data submitted by You do not contain any personal or sensitive data. You, therefore, acknowledge and agree that: (i) it is not the responsibility of Seqrite to verify the contents of Your submission while You access and use Seqrite Enterprise Mobility Management; (ii) Seqrite may share Your specimen submission or documentation with the information technology security fraternity and data associations; and (iii) You will not submit any personally identifiable or other sensitive information to Seqrite in any form whatsoever while submitting files and data on Seqrite Enterprise Mobility Management. The functionality of Seqrite EMM may differ based on device model and operating systems, and therefore, it is Your responsibility to evaluate the feature compatibility of Seqrite EMM against the technical specifications of Your device prior to availing license for Seqrite EMM. Seqrite expressly disclaims any liability arising out of Your failure to determine the interoperability of Seqrite EMM for Your device.

8. Seqrite Threat Intelligence (STI):

8.1 Introduction: Seqrite Threat Intelligence (STI) is an offering in the nature of portal based Software and may be hosted either in the customer premises or on cloud. STI aggregates, processes and disseminates cyber threat information with actionable insights suited to customer requirements.

8.2 Scope: Subject to the terms and conditions of the Agreement, Seqrite hereby : (i) grants You the access of STI; (ii) makes available to You, through STI, the threat intelligence data as collected from multiple open-source feeds and telemetry information of its products and as further processed or analyzed to filter inconsistency (**"Threat Feeds"**) by taking commercially reasonable efforts; and (iii) permits You to integrate the Threat Feeds with Your Pre-Existing Threat Feed (*as defined hereinafter*) or Your internal security controls. For the avoidance of doubt, it is explicitly clarified and agreed that it shall be Your sole responsibility to ensure the compatibility of Your systems and technical infrastructure with STI. Your access and use of the Feeds and related documentation shall be limited solely to Your own internal security purposes, and shall otherwise be subject to and in compliance with the terms and conditions of the Agreement and these Seqrite Product Specific Terms as applicable to STI. You are prohibited from reselling or otherwise distributing or disclosing Threat Feeds delivered through STI to any third parties except for limited disclosure to Your Authorized Users solely in connection with your internal security purposes. Unless expressly permitted in writing by authorized representative of Seqrite, You cannot : (i) redistribute, transfer, or resale Threat Feeds; and (ii) white-label or rebrand the backend platform embedded within the STI. All right, title and interest in and to the STI, Threat Feeds and related documentation, all copies and portions thereof, and all Updates, Upgrades or improvements, enhancements, modifications, any other inherent technology and all Intellectual Property Rights therein, shall at all times vest exclusively with Seqrite or the original licensor, as the case may be.

8.3 Your Pre-Existing Threat Feed: All right, title and interest in and to Your existing database of threat feeds, if any, which is input by You into the portal of STI or is otherwise supplied by You to Seqrite ("Your Pre-Existing Threat Feed") and all Intellectual Property Rights therein, shall at all times vest exclusively with You or Your original licensors, as the case may be. You hereby grant to Seqrite a non-exclusive, royalty-free, sublicensable, perpetual, irrevocable, assignable, transferable, worldwide right and license to use Your Pre-Existing Threat Feed to make available the Threat Feeds, develop and improve STI, and otherwise in its business as it determines in its discretion. You are responsible for Your Pre-Existing Threat Feed, including the means by which it is provided to Seqrite, and You shall be responsible for ensuring that Your Pre-Existing Threat Feed does not violate the intellectual property rights of any third party. You shall indemnify defend and hold harmless Seqrite, its Affiliate(s), directors, officers, employees, licensors, distributors, resellers and representatives of each of the foregoing from and against any claim, suit, action, penalties, losses, damages, fines, costs and expense (including reasonable attorney fees) arising out of or relating to Seqrite's use of Your Pre-Existing Threat Feed.

8.4 Limitations and Disclaimer: You acknowledge and agree that : (i) Threat Feeds may include references or hyperlinks to other websites or content over which Seqrite does not have any control; and (ii) Seqrite shall take commercially reasonable efforts to deliver the Threat Feeds by eliminating redundant duplicate information or otherwise reduce inconsistencies in connection with the Threat Feeds. Therefore, Seqrite does not guarantee that the : (i) uninterrupted, timely, error free and secure delivery of Threat Feeds; (ii) the accuracy, completeness and reliability of Threat Feeds or any of its output or other information ; and (iii) Threat Feeds shall be up-to-date. You assume all risk of damages of any kind arising out of or related to Your access to STI and use of Threat Feeds , including any reliance thereof. You acknowledge that by accessing STI and receiving Threat Feeds, You may be exposed to materials that are offensive, indecent, or objectionable, and under no circumstances shall Seqrite or its Affiliates be liable for such content. In addition to the foregoing, Seqrite or its Affiliates shall not be liable for any loss or damage caused by any technologically harmful material or viruses that may infect Your computer equipment, programs, information, data or other proprietary material, or that of any parties affected by Your actions due to Your access of the STI and use of Threat Feeds or any third party content or websites. Further, Seqrite shall also not be liable for defamation, libel or any other similar claim as a result of the content, notifications or alerts generated through STI or Threat Feeds. You understand that the Threat Feeds may contain malware, or other malicious content, and You agree not to use such content for malicious or unlawful purposes. You represent that You possess the requisite skills to safely handle such content. In the event You become aware or reasonably suspect that any person or entity is using the STI or Threat Feeds offering for any unlawful purpose, or to interfere with the security of STI or Threat Feeds, You shall immediately notify the same to Seqrite. Notwithstanding anything contained to the contrary in the Agreement and to the maximum extent permitted by applicable law, Your exclusive remedy and Seqrite's entire obligation and liability for the delivery, quality or accuracy of Threat Feeds, at Seqrite's discretion, shall be limited to reevaluate the Threat Feeds for eliminating the redundant duplicate information or reducing any inconsistences. Seqrite disclaims all other obligations and liabilities, or express or implied warranties regarding the Threat Feeds including implied warranties of merchantability, quality, fitness for a particular purpose, title, non-infringement, satisfactory quality or integration.

9. Seqrite Malware Analysis Platform (SMAP):

9.1 Introduction: Seqrite Malware Analysis Platform (**"SMAP"**) is an automated malware analysis system in the nature of portal based Software and may be hosted either in the customer premises or on cloud. You may upload or submit files such as executables (exe, dll,), windows documents, PDF and scripts (collectively, the **"Sample"**) on SMAP for scanning and analysing using the methods of submission as determined by Seqrite from time to time.

9.2 Limitations and Disclaimer: The Sample shall be scanned and analysed on the date and time determined by Seqrite. SMAP is provided on "AS IS" and "AS AVAILABLE" basis. Seqrite may commission or authorize third parties to carry out the scanning and analysis of Samples while providing access to SMAP. Seqrite reserves the right to remove any Sample without prior notice and at its sole discretion. In addition to the disclaimers of warranty as mentioned in the Agreement, Seqrite does not assure that a Report shall be generated for each file in the Sample or that SMAP will complete any analysis within any particular time frame or that the Report will be free of error or free of any defects. Seqrite neither assures any uptime for SMAP nor does it assure that the Report will be accurate or that SMAP will detect any malicious behaviour. Notwithstanding anything contained to the contrary in the Agreement and to the maximum extent permitted by applicable law, Your exclusive remedy and Seqrite's entire obligation and liability for Seqrite's liability for performance of SMAP, at Seqrite's discretion , shall be limited to reperforming the scan and analysis of Sample.

9.3 Your Representations and Warranties: By uploading or submitting the Sample on SMAP for the purpose specified herein, You represent and warrant to Seqrite that:

9.3.1 You have necessary rights to submit such Sample without breaching the rights of any third party, including intellectual property rights;

9.3.2 You shall provide such Sample that You wish to publicly share and that in any case, You shall not provide any Sample that is : (a) unlawful, pornographic or illicit material; (b) information that is confidential or proprietary to You; or (c) the personal data or information of any individual that You do not have the lawful permission to provide;

9.3.3 You shall use SMAP in accordance with applicable laws and not for any unlawful purpose;

9.3.4 You have the requisite skill to safely handle Malware;

9.3.5 You shall ensure that the security and confidentiality of the login credentials (i.e. username and password) of Your account on SMAP is maintained;

9.3.6 You shall notify Seqrite immediately upon learning, or otherwise having a reason to believe that a third party's rights to Sample, if any, that You have submitted have been violated;

9.3.7 You acknowledge to have exercised independent judgement in using SMAP and the Report, and have not relied either upon any representations made by Seqrite which have not been stated expressly by Seqrite herein or upon any descriptions or illustrations or specifications contained in any document, including catalogues or promotional material produced by Seqrite; and

9.3.8 You are solely liable for the Sample that You submit and all use thereof, including any dispute arising out of Your submission of Confidential Information and/ or personal data involved in the respective Sample; and Seqrite shall have no liability for such Sample or use.

9.4 SMAP Report: The analyses, reports, results and other output compiled and generated by SMAP, including without limitation, Seqrite's analysis of Sample (collectively "Report") is exclusively owned by Seqrite. Subject to the terms and conditions of the Agreement, Documentation and this clause of Seqrite Product Specific Terms, Seqrite grants to You a limited, non-exclusive, non-sublicensable and non-transferable license to access and use SMAP and the Report solely for Your internal business security. Notwithstanding the foregoing, You must not use SMAP and the Report for commercial purposes or for the benefit of any other third party. You grant Seqrite a non-exclusive, worldwide, royalty-free, irrevocable, transferable, sublicensable license to edit, host, store, reproduce, modify, create derivative works, communicate, publish, and distribute or otherwise commercially use solely the hash (MD5, SHA1,SHA256) of the Sample and its corresponding verdict post analysis for the purpose of enhancing Seqrite's internal threat intelligence and making the same available in offerings such as malware databases and reports.

9.5 Technical Support: The "Support " option on SMAP enables You to send queries directly to SMAP administrators. SMAP administrators shall revert to You over Your registered e-mail with response to queries raised by You.