AutoRek

Security Addendum

1 Introduction

The Parties agree that this AutoRek Security Addendum (**"Security Addendum"**) shall detail AutoRek's obligations with regards to security requirements throughout the Term of the Agreement. This Security Addendum is incorporated by reference into the Agreement and shall remain in effect for the duration of the Agreement.

2 Definitions

Capitalised terms used but not defined in this Security Addendum shall have the meaning given to them in the Agreement and Order Form as applicable.

Agreement:	the legally binding terms and conditions agreed between AutoRek and the Client (in relation to the use by the Client of Software Subscription Service) comprising the Software as a Service Agreement and any ancillary documentation referred to therein including any Order Form, and any SOW.

3 Security Requirements

3.1 AutoRek and any Material Subcontractors shall maintain ISO 27001 certification and AutoRek shall verify not less than annually the certification and credentials of the Material Subcontractors.

3.2 The following security measures apply to the Platform and all Environments unless otherwise specified.

4 Access Control

4.1 The Platforms shall be restricted to authorised users governed by an access control mechanism that supports; password complexity, password expiry, restrictions on password re-use, secure encrypted storage of user credentials.

4.2 The Software shall be restricted to authorised users governed by an access control mechanism that supports; password complexity, password expiry, restrictions on password re-use, secure encrypted storage of user credentials.

4.3 The Client is responsible for creation and management of end-user credentials to control access to the Software.

4.4 IP address whitelists will restrict internal communications and access by end-point IP addresses as specified by the Client from time to time.

5 Network Security

5.1 Platforms will be protected by firewalls with anti-malware protection including IPS/IDS.

5.2 Network logs shall be collected, securely stored and monitored for action and threat analysis.

5.3 DDoS protection will be applied to all production environments.

5.4 Endpoints shall be protected by anti-malware and file integrity monitoring solutions.

5.5 All devices shall be built, configured and hardened according to the applicable industry standards for such items.

5.6 External (to the Internet or any public network) web services published by the Software will be protected by web application firewalls.

6 Data Security

6.1 Endpoints within the platform shall be encrypted to AES 256 or better standards to provide at-rest data protection.

6.2 Backups shall be encrypted with AES 256 or better;

6.3 Data will be encrypted in transmission using TLS1.2 / AES 256 or equivalent.

7 Security Operations

7.1 Vulnerability scans shall be performed no less than every six (6) months, or upon material changes in the Platform.

7.2 Patch management shall be carried out to ensure all devices are routinely patched and a suitable patch management schedule shall be agreed with the Client.

7.3 SIEM shall be provided to gather, analyse, and respond to potential issues on a 24x7 basis.

7.4 Threat Intelligence monitoring shall be included in the operation of the Platform.

7.5 A penetration test of the Platform shall be conducted annually.

7.6 A penetration test and security review of the Software shall be undertaken at least annually.