MANAGED SECURITY SCHEDULE

1. DEFINITIONS

1.1. For the purposes of this Services Schedule, the following definitions shall operate in addition to and supplementary to those contained in the MSA, and ought to be read as if specifically incorporated therein:

1.1.1. "**Devices**" shall mean laptop computers, desktop computers and servers;

1.1.2. "**Endpoint Security**" means managed security for Devices, in the form of an advanced anti-virus solution through the RMM and shall comprise the managed Endpoint Security, or the managed Endpoint Security advanced, based on a Client's election, as set out more fully in clause 4 below;

1.1.3. "**MSA**" means the Master Services Agreement which is entered into by and between the Parties simultaneously herewith;

1.1.4. "**Network Edge Security**" means a firewall monitoring incoming and outgoing network traffic in order to protect an internal network from malicious traffic and viruses;

1.1.5. "**Proposal**" means the proposal to which this Services Schedule is annexed or to which the Proposal otherwise makes reference to, and which sets out, among other things, the exact nature of the Services required to be rendered, coupled with the cost in respect thereof;

1.1.6. "**RMM**" means the remote monitoring and management tool utilised in the provision of the Services;

1.1.7. "**Services**" means the managed security services, comprising of Endpoint Security Services and/or Network Edge Security Services based on a Client's election; and

1.1.8. "**Services Schedule**" means this document, which may be one of a series of Services Schedules, which is annexed to the Proposal.

1.2. In addition to the aforegoing, terms which are capitalised herein, but which have not been defined in clause 1.1 above, shall bear the same meaning as in the MSA.

1.3. Capitalised terms defined herein, but which also appear in the MSA, shall bear the meaning as defined herein.

2. INTRODUCTION

2.1. This Services Schedule is to be read with, and is subject to, the provisions of the MSA, and the Proposal to which this document is annexed. The Services Schedule is designed to define the Services to be rendered to the Client by the Service Provider.

2.2. This Services Schedule is the basis on which the Service Provider will perform the Services to the Client.

2.3. This Services Schedule may be coupled with any number of other Services Schedules as required for all services to be rendered to the Client.

3. NATURE OF THE SERVICES

3.1. The Services allow for Clients to ensure protection against viruses, malware, unauthorised access and the like in respect of their Devices and/or internal network.

4. ENDPOINT SECURITY SOLUTIONS

4.1. Endpoint Security shall consist of two levels, being managed Endpoint Security and managed Endpoint Security advanced. A Client may select, and which will be recorded in the Proposal, either one of these two levels in respect of all of their Devices. The Endpoint Security selection shall be provided on an either/or basis and not a mixed basis. As such, the selection as made shall be in respect of all Devices owned by a Client.

4.2. The Client will be provided with a non-exclusive, revocable software license, which is required strictly for the performance of Endpoint Security.

4.3. Endpoint Security is managed through the RMM, with any virus and/or possible attacks to a Device through a virus being automatically logged with the Service Provider's helpdesk.

4.4. Managed Endpoint Security and managed Endpoint Security advanced shall share a portion of the Endpoint Security base, being:

4.4.1. the scanning of files and drives on a Device;

4.4.2. incorporating of behavioural analysis to monitor the standard behaviour and function of the Device, enabling it to either block an activity or alert a Client in the event of such activity being outside of the normal parameters on the Device; and

4.4.3. inclusion of a ransomware agent which shall provide protection from any malware which may be used in transmitting data from, or encrypting files on a Device.

4.5. The managed Endpoint Security advanced shall in addition to the functions as set out in clauses 4.4.1 to 4.4.3 above include a complete disk encryption in respect of the Device thus preventing data access in the event of the Device being stolen. Decryption keys are stored within the RMM and may only be obtained by senior employees of the Service Provider with the appropriate access rights.

4.6. Should any Device have RMM uploaded on to it, and in instances where there are Devices without having Endpoint Security, the system will try detect this and it will be logged through the RMM and self-healing will attempt to deploy the Endpoint Security, with no guarantee of success being provided by the Service Provider.

5. NETWORK EDGE SECURITY

5.1. Managed Firewall:

5.1.1. The Managed Firewall Client Owned Equipment shall be supplied to a Client:

5.1.1.1. where the hardware is already owned by the Client and the Client hardware has a valid FortiCare license affiliated therewith; alternatively

5.1.1.2. in the event of the Client owning the hardware but the hardware does not have a valid FortiCare License.

5.1.2. Managed Firewall shall include the appropriate firewall hardware device together with the necessary license which shall be sold to the Client by the Service Provider.

5.1.3. In the event of the Client hardware not having a valid FortiCare license the Managed Firewall shall be a standard managed firewall Service and comprise of the following:

5.1.3.1. device management system;

5.1.3.2. provision of a virtual privacy network;

5.1.3.3. user authentication system;

5.1.3.4. daily configuration backups;

5.1.3.5. a policy audit check on a bi-annual basis; and

5.1.3.6. monthly reporting to a Client.

5.1.4. In the event of the Client hardware having a valid FortiCare License, the Managed Firewall shall be an advanced managed firewall Service and comprise of the Services set out in clause 5.1.2 above together with those set out below:

5.1.4.1. website filtering and control;

5.1.4.2. application detection and control;

5.1.4.3. an antivirus monitoring system;

5.1.4.4. device management system;

5.1.4.5. intrusion detection and prevention;

5.1.4.6. provision of a virtual privacy network;

5.1.4.7. user authentication system;

5.1.4.8. daily configuration backups; and

5.1.4.9. a policy audit check on a bi-annual basis.

5.2. Fully Managed Firewall:

5.2.1. The Fully Managed Firewall shall include the appropriate firewall hardware device together with the necessary license which shall be sold to the Client by the Service Provider.

5.2.2. The Fully Managed Firewall can further include, if so recorded and ordered as an optional extra in the Proposal, a Managed Wi-Fi component comprising:

5.2.2.1. 3 secure wireless access points;

5.2.2.2. installation of the Wi-Fi access points together with a single cable with a maximum length of 40 metres;

5.2.2.3. ceiling mount in respect of the access point; and

5.2.3. A standby unit to be made available to a Client should the unit at the Client's premises develop faults whilst under warranty, for the repair period of the original unit only.

6. GENERAL NETWORK EDGE SECURITY OFFERINGS

6.1. Any configuration changes required to be made in respect of the Managed Firewall shall be by written request from the Client with the Service Provider's helpdesk, and shall be attended to at the discretion of the Service Provider.

6.2. Where in respect of the Services set out in clause 5 above the bi-annual policy audit is in place, and action is required or amendments are suggested by the Service Provider, no such actions or amendments shall be effected, save as in consultation with the Client and on the specific instruction of the Client.

6.3. It shall be the Client's responsibility to inform the Service Provider of any and all changes made to a network (whether for a short period of time or by a permanent decommission) through which the Network Edge Security Services are provided so as not to compromise such Services, and further in order that, if necessary, all rules pertaining to the Device be removed from the firewall.

6.4. All abnormal activity on a Device, and through the firewall shall be monitored automatically and logged with the Service Provider's helpdesk and thereafter actioned for resolution. This abnormal activity shall include but not be limited to an infected Device attempting to transmit data, a high load being placed on the firewall, or repeated failed administrator logins.

6.5. Upgrades on the firmware comprising the Network Edge Security shall be attended to bi-annually on average. This is however subject to change based on whether stability issues in respect of updates are revealed, in which case the Service Provider may elect not to attend to an update in order not to damage the integrity of the Services, alternatively if it is revealed that there are bugs in the firmware then two or more upgrades may be necessary in any one year

7. INDEMNITY

7.1. The Network Security and Endpoint Security Services are designed to prevent infection of viruses, malware, ransomware and the like from entering an internal network and/or Devices, as the case may be.

7.2. Due to the development of new viruses and malware on a constant basis, the Service Provider unfortunately cannot and does not provide any guarantees that the Network Security and Endpoint Security Services will prevent the execution of any viruses, malware and ransomware on a constant basis.

7.3. As such, the Client hereby indemnifies and agrees to hold the Service Provider harmless in respect of any losses, damages or otherwise incurred, howsoever arising, suffered by the Client as a result of the failure of the Network Security and Endpoint Security Services.