Supplementary Terms - IT Support Services

The Services set out in these Supplementary Terms shall be supplied by Grant McGregor to the Client on the terms and conditions set out in Grant McGregor's General Terms and Conditions and those of these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

1.1 'Client Ticket' means the report of an Issue to Grant McGregor by the Client.

1.2 'Cloud-Based Utilities' means the collection of ancillary third-party provided services, including backup, anti-Malware, and Monitoring Services which will be used by Grant McGregor in support of the IT Support Services.

1.3 'Configuration' means the configuration of the IT Equipment or component thereof, including hardware, installed software and all associated settings and or parameters.

1.4 'Data Centre' means a remote data storage facility.

1.5 'Data Security Event' means a breach of the security of the Client's infrastructure resulting in loss or damage, including loss of user-names, passwords, Personal Data; crypto-locking or other Malware-related damage.

1.6 'Device' means an item of IT Equipment including Endpoints, tablets and mobile telephones.

1.7 'Endpoint' means IT Equipment which functions as a desktop workstation, which includes laptop computers, but excludes tablets and other mobile devices.

1.8 'End User' means a user of the IT Equipment.

1.9 'IT Equipment' means Servers, Endpoints, tablets and other devices and Software installed at the Client's Site, which is listed on the Order and is to be supported under the terms of this Agreement

1.10 'Hours of Cover' means the hours of cover set out in the Service Schedule, unless amended on the Order.

1.11 'IT Support Services' means on premise IT support services.

1.12 'Line of Business Applications' means the software which is installed on the IT Equipment and provided by the Client.

1.13 'Local Area Network' ('LAN') means the network infrastructure at the Client's Site.

1.14 'Malware' means software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system, including Trojan horses, viruses and ransomware.

1.15 'Monitoring Agent' means Software which is installed on the IT Equipment by Grant McGregor which enables system-monitoring and performance reporting.

1.16 'Monitoring Services' means Grant McGregor's Server monitoring, Desktop monitoring, network monitoring and / or backup monitoring services that remotely monitor the performance of Servers, Endpoints, Network Equipment and their operating systems.

1.17 'Network Equipment' means network equipment including routers, switches and wireless access points, but excluding cabling and cable systems.

1.18 'Public Internet' means the world-wide collection of private and public router-based networks that are interconnected via gateways and exchange points.

1.19 'Server' means IT Equipment which functions as a server; a single virtual server or a network attached storage server (file server).

1.20 'Service Component' means a component part of the Services.

1.21 'Response' means Grant McGregor's initial acknowledgement of a Client Ticket.

1.22 'Site' means Client's site at which IT Equipment is located, as set out in the Order.

1.23 'Software' means the software which is installed on and is a component of the IT Equipment, as listed on the Order.

1.24 'Service Desk' means Grant McGregor's dedicated team of qualified support technicians.

2. TERM

2.1 This Agreement will be deemed to come into effect on acceptance of the Client's Order by Grant McGregor and shall run until the RFS Date (the 'Run-Up Period') and following the RFS Date for a Minimum Term of twelve months unless otherwise set out in the Order.

2.2 This Agreement shall continue to run after the expiry of the Minimum Term (or subsequent Additional Term) for an Additional Term. The duration of the Additional Term shall be twelve months, unless otherwise set out on the Order. Grant McGregor shall, not less than ninety days prior to the end of the Minimum Term or any Additional Term thereafter, notify the Client of changes to charges and any other changes to the terms of this Agreement. In the event that:

2.2.1 The Client serves notice to terminate this Agreement in accordance with clause 11 of the General Terms and Conditions or clause 9 hereof, this Agreement shall terminate at the end of the Minimum Term or Additional Term thereafter;

2.2.2 The Client notifies Grant McGregor of acceptance of changes, the Agreement shall continue in force for an Additional Term;

2.2.3 The Client fails to notify Grant McGregor of acceptance of changes and fails to serve notice to terminate, such failure to notify Grant McGregor shall imply that the changes have been accepted and the Agreement shall continue in force for an Additional Term.

2.3 Notwithstanding the provisions of sub-clause 2.1, the Client may terminate this Agreement on written notice and without liability within ninety days of the RFS Date if the Client is not satisfied with Grant McGregor's performance of the Services.

3. PROVISION OF SERVICES

3.1 IT Support Services are provided to support the Client's IT Equipment. IT Support Services will be provided by Grant McGregor remotely and when required, visits shall be made to the Client's Site. For the avoidance of doubt, IT Support Services do not include the provision or support of network connectivity outside of the Client's Site, nor do the Services include maintenance of hardware, save warranty management and engineering activities that result there from.

3.2 The Services comprise IT Support Services as set out in the Order and described in the attached Service Schedule. Grant McGregor shall use reasonable endeavours to provide the IT Support Services during the Hours of Cover set out in the Schedule.

3.3 During the term of this Agreement, Grant McGregor shall be entitled to make alterations to the Configuration of the supported IT Equipment. Such alterations may result in temporary disruption to the availability of the IT Equipment and Grant McGregor will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

3.4 Grant McGregor cannot guarantee and does not warrant that the IT Support Services shall result in the IT Equipment operating free from interruptions or temporary degradation of the quality of the services provided by such IT Equipment.

3.5 If Grant McGregor provides services under the terms of this Agreement which rely upon Cloud-Based Utilities:

3.5.1 Grant McGregor shall use reasonable endeavours to provide the Cloud-Based Utilities 24 x 7 x 365;

3.5.2 Grant McGregor cannot guarantee and does not warrant that the Cloud-based Utilities will be free from interruptions, including:

a) Interruption of the Cloud-Based Utilities for operational reasons and temporary degradation of the quality of the Cloud-Based Utilities;

b) Interruption of the connection of the Cloud-Based Utilities to other network services provided either by Grant McGregor or a third party; and

c) Any such interruption of the Cloud-Based Utilities referred to in this sub-clause shall not constitute a breach of this Agreement.

3.5.3 Although Grant McGregor will use reasonable endeavours to ensure the accuracy and quality of the Cloud-Based Utilities, such Cloud-Based Utilities are provided on an "as is" basis and Grant McGregor does not make any representations as to the accuracy, comprehensiveness, completeness, quality, currency, error-free nature, compatibility, security or fitness for purpose of the Cloud-Based Utilities.

4. ACCEPTABE USE

4.1 The Client agrees to use the IT Equipment in accordance with the provisions of this Agreement, any relevant Service literature and all other reasonable instructions issued by Grant McGregor from time to time.

4.2 The Client agrees to ensure that the IT Equipment is not used by its End Users to:

4.2.1 Post, download, upload or otherwise transmit materials or data which is abusive, defamatory, obscene, indecent, menacing or disruptive;

4.2.2 Post, download, upload or otherwise transmit materials or data uploads or make other communications in breach of the rights of third parties, including but not limited to those of quiet enjoyment, privacy and copyright;

4.2.3 Carry out any fraudulent, criminal or otherwise illegal activity;

4.2.4 In any manner which in Grant McGregor's reasonable opinion brings Grant McGregor's name into disrepute;

4.2.5 Knowingly make available or upload file that contain Malware or otherwise corrupt data;

4.2.6 Falsify true ownership of software or data contained in a file that the Client or End User makes available via IT Equipment;

4.2.7 Falsify user information or forge addresses;

4.2.8 Act in any way which threatens the security or integrity of the IT Equipment, including the download, intentionally or negligently, of Malware;

4.2.9 Violate general standards of internet use, including denial of service attacks, web page defacement and port or number scanning;

4.2.10 Connect to the IT Equipment insecure equipment or services able to be exploited by others to carry out actions which constitute a breach of this Agreement including the transmission of unsolicited bulk mail or email containing infected attachments or attempts to disrupt websites and/or connectivity or any other attempts to compromise the security of other users of our network or any other third party system;

4.3 The Client acknowledges that it responsible for all data and / or traffic originating from the IT Equipment.

4.4 The Client agrees to immediately disconnect (and subsequently secure prior to reconnection) equipment generating data and/or traffic which contravenes this Agreement upon becoming aware of the same and / or once notified of such activity by Grant McGregor.

4.5 The Client agrees, subject to the provisions of sub-clause 10.13 of the General Terms and Conditions to indemnify Grant McGregor against all costs, damages, expenses or other liabilities arising from any third party claim which arises from the Client's breach of this clause 4.

5. THE CLIENT'S OBLIGATIONS

During the term of this Agreement, the Client shall:

5.1 Pay all additional Charges levied by Grant McGregor, including those arising from usage-based components of the Services.

5.2 Ensure that user-names, passwords and personal identification numbers are kept secure and:

5.2.1 On a regular basis, change access passwords for all IT Equipment that in the Client's reasonable opinion may be liable to access by unauthorised persons.

5.3 Agree that in all instances where it attaches equipment that has not been provided by Grant McGregor to the IT Equipment that such equipment shall be technically compatible and conforms to any instruction issued by Grant McGregor in relation thereto.

5.4 Accept that if it attaches equipment that does not comply with the provisions of sub-clause 5.4 ('Unauthorised Equipment') and such Unauthorised Equipment in the reasonable opinion of Grant McGregor is causing disruption to the functionality of the IT Equipment, Grant McGregor shall be entitled to:

5.4.1 If technically possible, reconfigure the Unauthorised Equipment, and charge the Client for its work at its prevailing rate;

5.4.2 Charge the Client at its prevailing rate for any additional work arising from, or in connection with the Unauthorised Equipment;

5.4.3 Request that the Client disconnect the Unauthorised Equipment from the IT Equipment; and if such request is not agreed by the Client within thirty days, terminate this Agreement forthwith.

5.5 Accept that is the Client's sole responsibility to take all reasonable steps, including the implementation of anti-virus systems, firewalls and staff training (where such are not provided by Grant McGregor under the terms of this Agreement) to prevent the introduction of Malware into the IT Equipment.

5.6 Be solely responsible for ensuring compliance with the terms of licence of any Software that is a component of the IT Equipment that has been provided by the Client.

5.7 Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the IT Equipment and any Cloud-Based Utilities provided by Grant McGregor.

6. GRANT MCGREGOR'S OBLIGATIONS

During the term of this Agreement, and subject to the performance by the Client of its obligations hereunder, Grant McGregor shall:

6.1 Provide the IT Support Services set out in the Order and described in the attached Service Schedule, subject to any service limitations set out in the Order and Schedule.

6.2 During the Hours of Cover, make available a Service Desk that shall provide support and guidance in the use of the IT Equipment and manage the resolution of all IT Equipment-related Issues raised by the Client, according to the Service Package set out on the Order.

6.3 During the hours of cover set out in the Schedule or as amended in the Order, monitor the performance of the IT Equipment, according to the Service Package set out on the Order.

6.4 Respond to Client Tickets raised by the Client and make reasonable endeavours to repair any Issue that is within the IT Equipment or directly caused by Grant McGregor, its employees, agents, subcontractors or suppliers.

6.5 Proactively respond to Issues reported by the Monitoring Services and make reasonable endeavours to repair any Issue that is within the IT Equipment.

7. Clause Intentionally Unused

8. GENERAL

8.1 During the term of this Agreement, the Client's suppliers will provide patches and maintenance releases ('Updates') for applying to the Software supported hereunder.

8.1.1 Grant McGregor shall, at the commencement of this Agreement agree an individual strategy for the application of Updates; and

8.1.2 The Client accepts that if it requests that Updates are not applied, there may be a resulting risk to the integrity of the IT Equipment and that Grant McGregor shall not be liable for any degradation in integrity resulting from such request; and

8.1.3 Grant McGregor shall immediately notify Client when Updates have been applied; and

8.1.4 The Client shall test its applications once the Update has been applied to ensure it has not impacted their services. If an Update has an adverse effect on the operation of the Software, Grant McGregor will where possible remove the Update, in agreement with the Client;

8.2 If the Client requires Updates to be applied to Line of Business Applications:

8.2.1 The Client shall be responsible for providing full installation instructions including any configuration details to Grant McGregor in advance;

8.2.2 The Client shall be responsible for notifying Grant McGregor of the availability of patches and maintenance releases to any Line of Business Applications which Client provides.

8.2.3 Grant McGregor shall install Updates to Line of Business Applications in response to specific requests from the Client, subject to fair usage. Grant McGregor shall be entitled to charge for the provision of this service, if, in its reasonable opinion, the number of requests made for such by the Client is excessive, the installation is complex and requires excessive work or if the Client requests that such service is to be provided outside of the hours of cover set out in the Order.

8.3 Grant McGregor may perform any Planned Maintenance that may limit the availability of the Cloud-Based Utilities. Planned Maintenance will be scheduled to minimise disruption to the Client. The Client will be notified at least forty eight hours prior to such Planned Maintenance taking place.

8.4 Grant McGregor will from time to time issue de-support notices against specific older versions of the installed Software products which form part of the IT Equipment. Such notices will be issued at least ninety days prior to the notice taking effect. During this period, Grant McGregor will provide an upgrade path in consultation with the Client.

8.5 Grant McGregor may be unable to provide prior notice of Emergency Maintenance, but will endeavour to minimise the impact of any such maintenance on the Client.

8.6 If Grant McGregor carries out work in response to an Issue reported by the Client and Grant McGregor subsequently determines that such Issue either was not present or was caused by an act or omission of the Client, Grant McGregor shall be entitled to charge the Client at its prevailing rate.

8.7 In the event of persistent breach of clause 4.2.8, Grant McGregor shall be entitled to:

8.7.1 Charge the Client at its prevailing rate for the removal of Malware;

8.7.2 Terminate this Agreement.

8.8 If the Client suffers a Data Security Event and subsequently requests assistance from Grant McGregor, it is the Client's sole responsibility to ensure that such request for assistance will not breach the terms of any cyber-insurance policy that the Client has in place, prior to requesting assistance from Grant McGregor.

8.9 If the Client is contacted by Grant McGregor and requested to make a change to the Configuration of the IT Equipment, it is the Client's sole responsibility to verify the identity of the requestor prior to carrying out the requested change.

8.10 If Grant McGregor resets any passwords during the execution of the Services, it shall be the Client's sole responsibility to change such changed passwords and ensure that such changes are compliant with any security policy that may be in effect.

8.11 The Client acknowledges that if it elects not to take advice in given by Grant McGregor in relation to the security and performance of the IT Equipment, there may be a resulting risk to the integrity of the IT Equipment and that Grant McGregor shall not be liable for any degradation in integrity resulting from such decision and that any additional costs incurred by Grant McGregor resulting there from will be charged to the Client.

8.12 The Client hereby consents to Grant McGregor and its sub-contractors accessing Servers and Endpoints that are supported under the terms of this Agreement.

9. TERMINATION

9.1 In addition to the provisions of Clause 11 of the General Terms and Conditions, this Agreement may also be terminated:

9.1.1 By either party by giving the other not less than ninety days' notice in writing to terminate at the end of the Minimum Term or any Additional Term thereafter;

9.1.2 By the Client by giving thirty days' notice in writing if Grant McGregor makes changes to the terms of this Agreement which are materially disadvantageous to the Client (for the avoidance of doubt, not including changes to charges) PROVIDED THAT such notice is given within thirty days of the effective date of the change(s).

9.2 On termination, howsoever caused, Grant McGregor shall be entitled to charge a termination fee ('Termination Fee'), which will cover Grant McGregor's costs of off-boarding the Client's End Users.

10. CHARGES AND PAYMENT

10.1 Fixed periodic Charges are based on the following:

10.1.1 Up to a maximum of four Servers;

10.1.2 One Endpoint per End User as set out on the Order;

10.1.3 All additional Servers, Endpoints and other Devices ('Additional IT') set out on the Order.

10.2 Invoices for fixed periodic charges shall be raised in advance of the relevant period. The invoicing period is set out in the Order.

10.3 In addition to Charges contemplated in sub-clause 10.1, Grant McGregor shall be entitled to charge the Client for:

10.3.1 The ad hoc supply of any Services that are requested by the Client but not set out on the Order;

10.3.2 Reasonable expenses;

10.3.3 Onsite visits that extend beyond the end of the Working Day

10.3.4 The Termination Fee, which shall be charged at Grant McGregor's prevailing daily charge rate and based on the number of End Users supported at the date of notification of termination:

a) 1.5 days for up to twenty five End Users;

b) 2.5 days for twenty six to fifty End Users;

c) 3.5 days for greater than fifty End Users.

10.3.5 End User administration in the event that the number of requests in any year exceeds ten percent of the number of End Users.

10.4 Grant McGregor shall commence charging for the IT Support Services from the RFS Date, regardless of the date on which the Client commences use of the IT Support Services. If the RFS Date does not correspond with Grant McGregor's invoicing period as set out in the Order, Grant McGregor shall charge the Client at a pro-rata rate for the first invoicing period.

10.5 The Client acknowledges that the Charges for the Minimum Term are calculated by Grant McGregor in consideration inter alia of the setup costs to be incurred by Grant McGregor and the length of the Minimum Term offered.

10.6 If, during the Minimum Term or Additional Term of this Agreement the Client requires additional End Users or equipment to be added to the Services, the Client shall raise a supplementary Order to cover the additional End Users and / or equipment and Grant McGregor shall promptly provide a quotation for the additional Services.

10.7 If the Client requests a reduction in the number supported End Users or quantity of IT Equipment during the Minimum Term:

10.7.1 The Client shall provide such request in writing, giving Grant McGregor not less than thirty days' notice;

10.7.2 Grant McGregor shall not unreasonably delay its acceptance of the Client's request;

10.7.3 The Charges for the remainder of the Minimum Term will be reduced but not below 80% of the amount agreed at the Commencement Date provided that the minimum number of supported End Users shall not be less than five.

10.8 If the Client requests a reduction in the number of supported End Users or quantity of IT Equipment during an Additional Term:

10.8.1 The Client shall provide such request in writing, giving Grant McGregor not less than thirty days' notice;

10.8.2 Grant McGregor shall not unreasonably delay its acceptance of the Client's request;

10.8.3 The Charges for the remainder of the Additional Term (and any subsequent Additional Term) will be reduced but not below 70% of the amount agreed at the Commencement Date provided that the minimum number of supported End Users shall not be less than five.

10.9 The IT Support Services will be provided by Grant McGregor for use by the Client on a fair use basis. If, in the reasonable opinion of Grant McGregor, the Client's use of the Services is deemed excessive, Grant McGregor and the Client shall discuss Grant McGregor's concerns and either agree a plan to reduce the excessive use of the Services or agree additional Charges to cover the cost of the excess use of the Services.

10.10 The Client agrees that it shall be liable for termination Charges if this Agreement is terminated by:

10.10.1 The Client terminating this Agreement for convenience prior to the end of the Minimum Term or any Additional Term, whereupon the Client shall be liable for the fixed periodic Charges payable for the remainder of the current term and the Termination Fee;

10.10.2 Grant McGregor terminating this Agreement prior to the end of the Minimum Term or Additional Term by reason of the Client's un-remedied breach of the terms of this Agreement, whereupon the Client shall be liable for the fixed periodic Charges payable for the remainder of the current term and the Termination Fee;

10.11 The Client shall not be liable for termination Charges if this Agreement is terminated by:

10.11.1 The Client at the end of the Minimum Term or end of any Additional Term PROVIDED THAT the Client properly serves written notice to terminate, in accordance with Clause 9 of this Supplement and Clause 11 of the General Terms and Conditions, though for the avoidance of doubt, the Client shall be liable for the Termination Fee;

10.11.2 Grant McGregor at any time if it can no longer provide the Services or part thereof;

10.11.3 The Client by reason of Grant McGregor's un-remedied or repeated breach of the terms of this Agreement;

10.11.4 The Client if Grant McGregor makes changes to the Services which detrimentally affect the Client PROVIDED THAT the Client complies with the provisions of sub-clause 9.1.2 hereof;

10.11.5 The Client if Grant McGregor makes changes the terms of this Agreement which are materially disadvantageous to the Client PROVIDED THAT the Client complies with the provisions of sub-clause 9.1.2 hereof;

10.11.6 The Client under the terms of sub-clause 2.3, in which case Grant McGregor will refund all Charges paid to date by the Client

11. LIMITATIONS AND EXCLUSIONS

11.1 In addition to the terms set out in clause 12 of the General Terms and Conditions, Grant McGregor shall also be entitled to suspend the provision of Services, in whole or part, without notice due to Grant McGregor being required by Government, emergency services, regulatory body or other competent authority to suspend Services.

11.2 Whilst Grant McGregor's Monitoring Service is intended to proactively identify most system-related issues, Grant McGregor does not warrant and cannot guarantee that the Monitoring Service will identify all system-related issues and shall not be liable for any losses, damages or costs unless such result directly from the negligence of Grant McGregor.

11.3 Grant McGregor shall not be liable for any damage or costs resulting from a failure of an update to anti-Malware software, failure to detect Malware or incorrect identification of Malware, unless such failure is caused by the negligence of Grant McGregor.

11.4 Grant McGregor shall not be liable for any damages, costs or charges arising from damage to, or theft of backup data that is transmitted from the Client's Site to the Data Centre via the Public Internet, nor for any other losses that occur due to reasons beyond its reasonable control.

11.5 The Services provided by Grant McGregor under the terms of this Agreement are solely IT Support Services and do not include:

11.5.1 The resolution or remediation of consequences of Data Security Events;

11.5.2 The investigation of the causes of Data Security Events.

11.6 In the event of data loss by the Client (whether caused by a Data Security Event or any other reason), Grant McGregor's responsibility shall be limited to restoration of the latest backup of the applicable data.

11.7 Grant McGregor will not provide warranty management for hardware components of the IT Equipment that are no longer supported by their vendors.

11.8 This Agreement does not include:

11.8.1 The support of any equipment that is not listed on the Order;

11.8.2 Repair or replacement under manufacturer's warranty of any damaged IT Equipment where such damage is caused by accident, misuse or wear and tear;

11.8.3 The supply of any consumables;

11.8.4 Any form of hosting, save backups;

11.8.5 Recovery of Client data whose loss can be reasonably attributed to accidental deletion, mis-use or negligence by the Client;

11.8.6 Maintenance of structured cabling including cabling, patch panels and wall sockets;

Grant McGregor may at its sole discretion provide any of the excluded services listed in the sub-clause 11.8, and charge for the supply thereof at its prevailing rate.

11.9 During the resolution of an Issue Grant McGregor will provide on-site support at its sole discretion.

11.10 The Client acknowledges and agrees that:

11.10.1 Any recommendations or advice provided by Grant McGregor is intended merely to mitigate the Client's cyber vulnerability and is provided without any warranty that that on implementing such recommendations or advice, the Client will be free from cyber security vulnerabilities or their attendant risks;

11.10.2 Grant McGregor shall not be liable for any liabilities, losses, damages, costs, fines or expenses that result directly or indirectly from recommendations or advice provided by Grant McGregor unless such recommendation or advice was either given negligently or was negligently withheld.

11.11 All Cloud-Based Utilities are provided on an 'as is' basis, without warranty, guarantee of fitness for purpose or suitability for the Client's purpose; and

11.11.1 Grant McGregor shall not be liable for any damages or costs arising from a failure of any component of the Cloud-Based Utilities, including failure to detect Malware, Data Security Events or the requirement for security updates unless such failure is caused by the negligence of Grant McGregor.

11.12 Software updates are supplied by Grant McGregor-authorised software vendors and not Grant McGregor. Grant McGregor will use reasonable endeavours to prevent a Software update causing an adverse reaction with any particular equipment configuration; however Grant McGregor shall not be liable for any disruption resulting from the installation of Software updates. In such circumstances, Grant McGregor's sole responsibility will be to de-install the Software update or roll back to an appropriate restore point to resolve the issue.

Service Schedule

Grant McGregor offers a number of different Service Packages. Each of the Service Packages offered by Grant McGregor is described in this Schedule and in addition, each of the Service Components which make up the various Service Packages is described in more detail. The actual Service Package(s) that are subscribed to by the Client are listed on the Order.

1. Service Package Summary

This paragraph summarises each of the Service Packages offered by Grant McGregor. The individual Service Components listed in each Service Package are more fully described in the following paragraphs.

Single Gold Standard Support Service
• Service Desk • Monthly Reporting • Client Satisfaction Scoring • Mobile Device Management • Server, Virtual Server and NAS System Monitoring and Management • End User Device Monitoring and Management • Basic Network Monitoring • Software Update Service • Software Installation Service • User Administration • IT Supported Asset Register • Hardware Update Service • Third Party Liaison • Quarterly Business / Technology Review

Essential Security Services
• Antimalware and Antivirus Protection • Managed Threat Protection & Zero Trust Service • Advanced Web Filtering • Endpoint Device Control (USB) • Desktop Firewall

Optional Support / Security Services

Optional Support / Security Services

• Advanced Network Monitoring Service
• Line of Business Software Updates
• Professional Services
• Backup Service for Microsoft 365
• Managed Data Backup and Disaster Recovery Service
• Enhanced Security, including
  • Security Risk Assessment
  • Antimalware and antivirus
  • Advanced Threat Protection
  • Multi-Factor Authentication
  • Security Awareness Training
  • Dark Web Monitoring
• Advanced Email Security, including
  • Real Time Threat Mitigation
  • Email Continuity
  • Email Archiving
  • Email Encryption

2. Single Gold Standard Service

2.1 Service Desk

Subject to fair usage, there are no restrictions on the number of Client Tickets that the Client can raise with Grant McGregor's Service Desk. The Service Desk provides support and assistance in the use of the IT Equipment, including the following:

- Management of the prompt resolution of Issues within the IT Equipment that are identified by the Client
- Provision of help and guidance in the use and configuration of the IT Equipment
- Remote access to facilitate Issue resolution if possible and appropriate
- Subject to fair usage, there are no restrictions on the number of on-Site visits that Grant McGregor will make to support the IT Equipment during the Working Day if it is not possible to resolve an Issue remotely, however Grant McGregor may, under certain circumstances make a charge for its travelling expenses
- Escalation management if required in the event of protracted Issue resolution
- Management of Change Requests
- Third party escalations and management

2.1.1 The Service Desk is available during the 8am to 6pm Monday to Friday excluding Scottish bank and public holidays;

2.1.2 The Client can make requests for assistance by one of the following methods:

- By Email to Grant McGregor's Service Desk – servicedesk@grantmcgregor.co.uk
- By Telephone to Grant McGregor's Help Desk – 0131 603 7911
- Web Chat via Grant McGregor's website www.grantmcgregor.co.uk
- Via Grant McGregor's support portal – http;//remote-portal.co.uk

2.1.3 The Client can raise Tickets at any time by email though such Client Tickets will only be responded to during the Working Day.

2.1.4 Grant McGregor will endeavour to respond to Client Tickets within the timescales set out in paragraph 5.

2.2 Service On-boarding

2.2.1 Grant McGregor will review and where necessary make appropriate changes to the IT Equipment's configurations to ensure that the Services detailed in this Schedule can be delivered effectively. This will include but is not limited to the configuration of Microsoft Windows event logs, Microsoft Windows, Exchange and SQL Server services, anti-virus software and backup software.

2.2.2 Grant McGregor will make recommendations about the data that is included or excluded as part of the Client's backup configuration, but is not responsible for these decisions or for the ongoing maintenance of the backup sets.

2.2.3 Grant McGregor will agree with the Client a number of standard procedures that Grant McGregor will follow when receiving requests from the Client for adding, removing or changing access to the Clients

network. This will include but is not limited to creating, deleting, or amending user accounts, security permissions, and folders and shares.

2.2.4 Grant McGregor will inform the Client if Grant McGregor is unable to configure any components the IT Equipment to provide the necessary alerting and will agree a suitable alternative with the Client.

2.2.5 Grant McGregor will document the Client's IT infrastructure, identify the roles of each component of the infrastructure and provide the Client with a copy of the documentation;

2.3 Server Monitoring and Management

Grant McGregor will install its Monitoring Agents on the Servers set out on the Order to enable pro-active monitoring. The Monitoring Agents will monitor key aspects of system performance and will alert Grant McGregor to any detected or potential Issues. The Monitoring Agents will monitor Server and Endpoint performance 24 x 7 x 365 and automatically resolve Issues whenever possible. Grant McGregor shall respond to any alerts that cannot be automatically resolved during Service Desk Hours of Cover in a manner that is appropriate to the severity of the alert, whilst aiming to minimise disruption to the availability of the monitored Servers and Endpoints. Remote monitoring shall be restricted to Servers which support SNMP and/or ICMP packets. Grant McGregor shall:

- Monitor processor, memory and hard disk usage and performance of all Servers to help to prevent system downtime or performance degradation
- Monitor the critical services that are necessary to help to maintain the effective performance of the Server operating system(s)
- Monitor the Windows event logs against Grant McGregor's current list of monitored events (including those which indicate a pending or current Hardware failure) to help to prevent system downtime or performance degradation
- Diagnose and remediate Issues
- Maintain group security policy
- Maintain End User, Hardware and Software asset registers
- Install white-listed patches as they are made available for the vendor-supported operating systems and applications listed below. Where a Server re-boot is required to complete patch installation, this will be carried out outside of the Working Day
    - Windows Server operating systems
    - Microsoft Exchange
    - SQL Server

2.4 Endpoint Monitoring and Management

Grant McGregor will install its Monitoring Agents on the Endpoints set out on the Order to enable pro-active monitoring. The Monitoring Agents will monitor key aspects of system performance and will alert Grant McGregor to any detected or potential Issues. The Monitoring Agents will monitor Endpoint performance 24 x 7 x 365 and automatically resolve Issues whenever possible. Grant McGregor shall respond to any alerts that cannot be automatically resolved during help desk Hours of Cover in a manner that is appropriate to the severity of the alert, whilst aiming to minimise disruption to the availability of the monitored Endpoints. Remote monitoring shall be restricted to Endpoints which support SNMP and/or ICMP packets. Grant McGregor shall:

- Monitor processor, memory and hard disk usage and performance of all Endpoints to help to prevent system downtime or performance degradation
- Monitor the critical services that are necessary to help to maintain the effective performance of the Endpoint operating system(s)
- Monitor the Windows event logs against Grant McGregor's current list of monitored events (including those which indicate a pending or current Hardware failure) to help to prevent system downtime or performance degradation
- Diagnose and remediate Issues
- Install white-listed patches as they are made available for the vendor-supported operating systems and applications listed below. Where a Server or Endpoint re-boot is required to complete patch installation, this will be carried out outside of the Working Day
    - Windows Endpoint operating systems
    - Apple Endpoint operating systems
    - Microsoft Office
    - Microsoft Browser

- Chrome Browser
- Safari Browser
- Firefox Browser
- Adobe Reader

2.5 Basic Network Monitoring

Grant McGregor will provide, during the Working Day:

- Basic SNMP network monitoring, including manufacturer-supported routers, switches, firewalls and wireless access point connections
- Network trouble-shooting and performance / fault diagnosis and remediation
- Updates to Network Equipment configurations
- Firmware and security updates and their installation

2.6 Mobile Device Management

Grant McGregor's mobile device application support covers support for the configuration of:

- Microsoft 365 Email
- SharePoint
- Microsoft Office 365 OneDrive
- Outlook
- Excel
- Word
- PowerPoint
- Teams
- Microsoft Authenticator
- Duo 2FA
- Adobe Reader
- Safari browser
- Google Chrome browser

Mobile device operating system support and management is provided via a Grant McGregor-supplied Microsoft InTune subscriptions or other Grant McGregor-supplied MDM software subscription. Mobile device management includes:

- Enrolment of devices and End Users
- Publishing security settings, certificates and profiles to devices
- Resource access control
- Monitoring and management, including measuring and reporting device compliance and app inventory
- Publishing mobile apps to devices
- Configuration of email applications
- Securing and removal of corporate data

Mobile device management does not include the publishing or management of anti-Malware software or hardware support for physical devices.

2.7 User Administration

Grant McGregor will ensure that Server-based End User accounts are at all times properly managed and in response to specific requests made by the Client:

- Activate / deactivate software licences
- Update Microsoft Windows and Azure Active Directories to add / remove or change user accounts,

- Set up / remove email accounts, data folders and shares, and the related security permissions
- De-provisioning and re-provisioning existing Endpoints and other devices

This service is provided subject to the number of requested changes not exceeding 10% of the size of the Client's End User base. Grant McGregor will be entitled to charge the Client for changes in excess of this limit. If the Client requests updates to Global Security Clients, Grant McGregor will charge for such changes at its prevailing rate.

2.8 Third Party Liaison

Grant McGregor will provide up to a maximum of two hours per month for liaison with suppliers of software, equipment and services that have not been provided by Grant McGregor. Examples of such include Public Internet connectivity issues and Line of Business Application issues. If the Client requires more than two hours' assistance, Grant McGregor will provide such and will charge at its prevailing rate. Time that is unused in any month cannot be rolled forward.

2.9 Hardware Update Service

Grant McGregor will once a quarter provide firmware, BIOS and driver Updates for Grant McGregor-supplied Hardware that is covered by its manufacturer's warranty or extended warranty, including Servers, Endpoints and Network Equipment but not including tablets or other mobile devices. Most Updates will be applied remotely; if site visits are required to upgrade Endpoints, such visits will be chargeable at Grant McGregor's prevailing rate. If updates are required more frequently than once a quarter, Grant McGregor will make an additional charge.

2.10 Software Installation Service

Grant McGregor will provide up to a maximum of two hours per month for the installation or de-installation of Line of Business Software. If third party support of the installation is required, such support will count towards the two hour limit. Time that is unused in any month cannot be rolled forward. Larger software installations can be undertaken and will be treated as professional service projects.

2.11 Monthly Reporting

Grant McGregor will provide monthly reports which include:

- Service metrics (Issues raised, resolved, resolution performance against SLA)
- Client satisfaction scores
- Users and active system accounts
- Supported Hardware – asset register
- Installed supported software – asset register
- Server performance / availability
- Patch update status

2.12 Quarterly Business / Technology Review

Grant McGregor will undertake quarterly business / technology review meetings with the Client's senior management and decision makers, with the purpose of:

- Assisting with the road-mapping of the Client's IT strategy
- Advising on current landscape and technology changes
- Offering input to future strategy and budgeting
- Discussing and understanding any ongoing issues with the Client
- Analysing Service Requests, checking for patterns to help identify root causes
- Understanding the Client's business requirements to determine recommendations and changes where appropriate

3. Essential Security Services

3.1 Virus and Malware Protection

3.1.1 Grant McGregor will provide industry standard an anti-malware service for all Endpoints and Servers. Grant McGregor's anti-malware service is focussed on security and speed. It employs a unique approach to virus / malware protection and is largely cloud-based. This approach means that its monitoring and detection are carried out with very little performance impact compared with other anti-virus / anti-malware software

and obviates the need for constant updating of Endpoints or Servers with virus definitions. The service includes:

- Real-time threat protection
- Anti-phishing filter

3.1.2 Grant McGregor will:

- Schedule regular anti-Malware scans all Endpoints and Servers
- Monitor Endpoints and Servers on a daily basis to ensure that protection remains active and automatically raise an alert if protection is disabled

3.1.3 If the Client accidentally introduces Malware onto the IT Equipment, Grant McGregor shall attempt to remove such Malware; in the first instance the anti-malware service will attempt disinfection and removal. If the automated disinfection and removal fails, Subject to the following, Grant McGregor will attempt to manually disinfect and remove the Malware and if that fails, will re-install operating systems, applications and last known data backups:

a) All work will be carried out during the Hours of Cover;

b) If more than 10% of the Endpoints are affected, Grant McGregor will charge at its prevailing rate for restoration of the Endpoints (whether successfully manually restored or re-installed);

c) Any time spent investigating the attack or further consequences shall be charged at Grant McGregor's prevailing rate;

d) This undertaking is however subject to the provisions of sub-clauses 8.7 and 8.8 of these Supplementary Terms.

3.2 Managed Threat Protection & Zero Trust

Grant McGregor's Managed Threat Protection & Zero Trust Service is based on a layered next-generation platform with prevention, detection and blocking capabilities, using proven machine learning techniques, behavioural analysis and continuous monitoring of running processes which:

- Provide a multi-layered next-generation security solution, which provides detection and remediation against all kind of threats
- Use machine learning, advanced heuristics, advanced anti-exploit and other proprietary techniques to protect the Client's IT Equipment
- Provide proactive hardening and risk analytics to reduce the attack surface
- Provide network based security to stop attacks aiming to gain access to the system by exploiting network vulnerabilities

The service uses machine Learning anti-Malware Machine learning techniques to predict and block advanced attacks. The service's machine learning models use 40,000 static and dynamic features and are continuously trained on billions of clean and malicious file samples gathered from over 500 million endpoints globally, which dramatically improves the effectiveness of Malware detection and minimizes false positives.

The included process inspector operates in zero-trust mode, continuously monitoring all processes running in the operating system. It hunts for suspicious activities or anomalous process behaviour, such as attempts to disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation), replicate, drop files, hide from process enumeration applications and more. The service takes appropriate remediation actions, including process termination and undoing changes the process made. It is highly effective in detecting unknown advanced Malware.

Exploit prevention technology protects the memory and vulnerable applications such as browsers, document readers, media files and runtime (for example Flash, Java). Advanced mechanisms monitor memory access routines to detect and block exploit techniques such as API caller verification, stack pivot, return-oriented-programming and others. The service is equipped to tackle advanced, evasive exploits that targeted attacks rely on to penetrate an infrastructure.

3.3 Web Threat Protection and Content Filtering

Grant McGregor's advanced web filtering service creates a barrier between the Client's network and the Public Internet, limiting and where possible preventing access to the Client's systems by intruders and helping to prevent the unintentional downloading of Malware, as well as preventing End Users from browsing selected websites. The service is underpinned by an advanced, self-learning, remote software platform which continually analyses security threats and the relationships between them and builds an always up to date holistic view of the security threat landscape. The service enables Grant McGregor to provide enhanced, real time control of the Client's End User access to the internet from all Endpoints. The creation, application and management of the rules which allow End Users to interact with the Public Internet whilst affording the maximum level of protection for the Client's network is a complex task, and is fully undertaken by security specialists at Grant McGregor. Grant McGregor will:

- Install its advanced web filtering agents on each Endpoint, which will afford protection whether the Endpoint is connected to the Public Internet via the Client's LAN or via any other method of access;
- In response to specific requests from the Client, implement the restriction of access to specific websites or categories of websites.

3.4 Endpoint Device Control (USB)

Grant McGregor's Endpoint Device Control Service helps to prevent data leaks and malware infections by managing access to devices connected to the Client's Endpoints. Device access is managed through rules and exclusions via a configurable policy, for example:

- Allowed: the device can be used on the target Endpoint
- Blocked: the device cannot be used on the target Endpoint
- Read-Only: only the read functions can be used with the device
- Custom: define different permissions for each type of port from the same device, such as Firewire, ISA PnP, PCI, PCMCIA, USB

3.5 Desktop Firewall

Grant McGregor will install and configure Desktop firewall software and its updates, which in addition to providing an additional level of protection whilst such Equipment is located on the Client's Site will provide protection when Equipment is used remotely from the Client's Site.

4. Optional Services

Optional Services will be provided if set out on the Order or if appropriate on an ad hoc basis in response to supplemental Orders / individual requests raised by the Client.

4.1 Advanced Network Monitoring

Grant McGregor's network monitoring service is a powerful platform for managing Network Equipment for ensuring optimal network performance and reducing the risk of service impact due to network related issues.

4.1.1 Network topology maps are automatically generated and maintained along with device configuration backup and configuration change notification and comparison.

4.1.2 The network monitoring service provides an invaluable troubleshooting capability for identifying issues such as network congestion, broadcast traffic, packet errors and discards along with CPU & memory issues on any managed network device.

4.1.3 Grant McGregor will undertake monthly trend analysis and reporting on the network infrastructure in addition to scheduling annual firmware upgrades for all managed network devices.

4.1.4 Grant McGregor's Monitoring Agent will scan for managed Network Equipment which will automatically be added to the service. This includes managed switches, routers, firewalls, wireless access controllers & wireless access points. Unmanaged devices will not be added to the service and will not be charged.

4.1.5 Hardware maintenance / manufacturer's warranty is required to be in place on all Network Equipment that is covered by Grant McGregor's advanced network monitoring service.

4.1.6 Grant McGregor shall provide the following services:

- Automated network mapping
- Automated inventory
- Network documentation
- IP address management
- Alerts and notifications
- Service monitoring
- Usage and health statistics
- Live and historic data
- Traffic insights
- Quality of Service reporting
- Automated self-healing
- Network evidence
- Configuration management
- Configuration restore
- Configuration analysis

4.1.7 Grant McGregor's Network Management Service does not include:

- Identifying every device discovered on the network
- Configuring Windows Management Instrumentation
- Wireless security scans for rogue access points or other issues

- Network reconfiguration

4.2 Line of Business Software Updates

If requested and it is possible to automatically apply Line of Business Software Updates, Grant McGregor will install Line of Business Software Updates. If the installation of any particular Update requires additional time or resource beyond that which Grant McGregor reasonably expects and charges for, Grant McGregor will be entitled to charge the Client any additional effort required to carry out the installation.

4.3 Professional Services

Grant McGregor will provide design, installation and configuration services as a discrete assignment, either prior to, during, or independent of the delivery of the Services described in this Schedule. Grant McGregor will charge the Client for the supply of these services at its prevailing rate.

4.3.1 Design Services

Design services include assessment of the Client's requirement and the design of a solution, including, as appropriate, server architecture, software, configuration, local and wide area networks. Further design services may be provided in response to change requests. Grant McGregor will produce a detailed proposal ('Proposal') which will set out the proposed architecture and will include any additional costs, for agreement with the Client prior to implementation.

4.3.2 Site Surveys

Site surveys will be provided as required and further site surveys may be provided in response to change requests.

4.3.3 Project Management

Grant McGregor will project manage the assignment using its preferred management methodology. Project management activities shall include project planning, project/milestone reviews with the Client, change request management, issue management, configuration management, project reporting and supplier management including liaison with suppliers of hardware and enabling services.

4.3.4 Procurement and supply of hardware and software

If agreed, Grant McGregor will procure hardware and software from its suppliers, if required stage the hardware and deliver it to the Client's Site.

4.3.5 Installation and configuration of hardware and software at the Client's Site

Grant McGregor will install and configure hardware and software at the Client's Site, on the dates agreed. If the proposed installation is expected to require less than two hours' work, Grant McGregor may at its discretion, waive its charges.

4.3.6 Commissioning and testing

Prior to handover to the Client, Grant McGregor shall test the full installation, address any non-conformity and ensure that the installed hardware and software is performing to expected standards. Grant McGregor will furnish the Client with copies of all test results.

4.3.7 Acceptance Testing and Acceptance

The Client shall be responsible for carrying out its own acceptance testing / acceptance testing against its acceptance criteria. The Client shall, within 30 days of handover, either sign Grant McGregor's Acceptance Note or advise Grant McGregor of any non-conformances that it has identified, whereupon Grant McGregor shall address all outstanding non-conformances.

4.3.8 Floor Walking / Dedicated Technician

Grant McGregor will provide a dedicated on-site engineer for the number of days / half days set out on the Order. Whilst on site the engineer will be available to provide support to End Users as required. This service is intended to provide support, not development activities.

4.3.9 Strategy & Planning

Grant McGregor will provide consultancy to help the Client to plan and develop its information technology to ensure that its information technology is strategically transformational and enabling. This service is provided in addition to initial on-boarding and quarterly business reviews described in paragraphs 2.2 and 2.11 respectively.

4.4 Backup Service for Microsoft 365

Grant McGregor's backup service for Microsoft 355 protects the Client against loss of data that is held within Microsoft's cloud infrastructure. Unexpected data loss can typically be due to user error or occur if an End User subscription expires, and Grant McGregor's service, in addition to providing the Client with additional control over its data, mitigates the risk of such data loss.

4.4.1 Grant McGregor will back-up the Client's Microsoft 365 data based on the number of active End Users. Backup data is stored at Grant McGregor's EEA-based Data Centre;

4.4.2 Microsoft 365 backups include:

- OneDrive file and folder data backups (documents), per End User
- Exchange data, including emails, email attachments, notes, deleted items, contacts (excluding photographs), tasks and calendar events (including attendees, recurrence, attachments and notes)
- SharePoint primary, custom, group and team site collections; folders, document libraries and sets site assets, templates and pages
- Groups (including conversations, plans, files, sites and calendar)
- Teams (including wiki and chat)
- Audit logs, data controls and export capabilities

4.4.3 Backups will be made daily;

4.4.4 The Backup and Recovery Service is fully managed by the Grant McGregor;

4.4.5 The backup system will automatically notify Grant McGregor of backup success or failure;

4.4.6 Backups are encrypted at rest and during transmission;

4.4.7 Grant McGregor will retain backup data as set out on the Order;

4.4.8 Data restoration:

- Data restores will only be initiated by Grant McGregor when requested by an authorised representative of the Client
- Grant McGregor will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level) requested by the Client
- Grant McGregor will use reasonable endeavours to restore data to the location that is specified by the Client

4.4.9 Whilst Grant McGregor shall execute automatic backups and monitor the performance of the backup service 24 x 7 x 365, Grant McGregor will carry out the following activities during the Working Day:

- Respond to Client requests for data restores;
- Respond to and investigate any Issues that arise in the service which cannot be remediated automatically, whether raised by the Client or by Grant McGregor's Monitoring Agent.

4.5 Managed Data Backup and Disaster Recovery Service

4.5.1 Grant McGregor will back-up the Client's Servers and Endpoints, as set out on the Order.

4.5.2 Endpoint backup data is stored:

- At Grant McGregor's EEA-based Data Centre; or
- If set out on the Order, a Data Centre nominated by the Client

4.5.3 200GB of data storage per Endpoint is included in the service; additional charges will be made per additional GB or part thereof.

4.5.4 Server backup data is stored:

- At Grant McGregor's EEA-based Data Centre; or
- If set out on the Order, a Data Centre nominated by the Client
- And if set out on the Order, on a local network attached storage device

4.5.5 1000GB of data storage per Server is included in the service; additional charges will be made per additional GB or part thereof.

4.5.6 The Backup and Recovery Service is fully managed by Grant McGregor;

4.5.7 The backup system will automatically notify Grant McGregor of backup success, backup errors and backup failures;

4.5.8 In the event of a Backup Failure:

- If a backup failure is detected by Grant McGregor's monitoring system, the backup system will automatically attempt to complete the backup during the next scheduled backup window
- If the backup fails 2 consecutive times Grant McGregor's support team will receive an alert from the backup system and will investigate the problem to identify the root cause

4.5.9 Backups are encrypted at rest.

4.5.10 Backups are made daily and the retention period is set out on the Order. Additional retention periods are available upon request and should be specified on the Order or requested as a Change Request; and Initial full backups will be made on commencement of the Services and if deemed necessary by the backup service itself following the re-boot of any backed-up Server.

4.5.11 Data restores are only initiated when requested by the Client; and

- Data can be restored at various levels of granularity, including image, directory or file level, as requested by the Client
- Grant McGregor shall charge for providing data restores at its prevailing rates

4.5.12 Following a disaster, full Server images can be restored onto the Client's original Server or onto virtual servers on alternative, Client-supplied hardware; and

- Grant McGregor will execute a test disaster recovery invocation during installation of the backup and disaster recovery service
- Grant McGregor will, on request by the Client, execute additional disaster recovery invocations and charge for such at its prevailing rate

4.6 Enhanced Security

4.6.1 Security Risk Assessment

Grant McGregor will on a regular basis carry out automated Cyber-security Assessments which provide the Client with a risk- and fact- based view of the challenges and opportunities associated with cyber-security and help address rapidly changing threats and risks. The Security Risk Assessment will be carried out on the Client's on-site, cloud or hybrid infrastructure. Grant McGregor collects relevant information through an automated survey that uses agents which delete themselves following the Endpoint scan. The agent:

- Searches content in Office 365 and SharePoint for personally identifiable information. Access granted to SharePoint sites and documents is also extracted. This is then compared with the accounts in the active directory to identify potential for unauthorised access
- Collects information relating to local accounts, firewall rules, applications installed, the operating system, installed service packs, shares and the registry from Windows OS-based Endpoints in the Client's IT infrastructure
- Retrieves user and group information, identifies external users and (unused) accounts (including admin accounts) and reports suspicious accounts
- Discovers registered mobile devices from Intune

Grant McGregor will identify areas requiring attention and recommend action to be taken.

4.6.2 Antimalware and Antivirus Service

Grant McGregor's Antivirus and Antimalware Service provides clear visibility into indicators of compromise and threat investigation and incident response workflows. The integrated Endpoint data recorder performs a broad capture of system activities including file & process, program installation, module loads, registry modification, network connections, which provides an enterprise-wide visualization of the chain of events in the attack. The threat analytics module continuously sifts through behavioural events in system activities and creates a prioritised list of incidents for additional investigation and response. Only relevant, correlated and high severity-rated events are presented for manual analysis and resolution. Noise and redundant information is kept to a minimum, as the vast majority of attacks and advanced attacks are blocked at the pre-execution or on-execution stages. Elusive threats, including file-less Malware, exploits, ransomware and obfuscated Malware, are neutralized by the highly effective layered next generation Malware prevention technologies and an on-execution behaviour-based process inspector. Automatic response and repair eliminate the need for human intervention in blocked attacks.

The Service provides:

- Insight into suspicious activities and indicators of compromise
- Integrated hardening, Endpoint protection and Endpoint detection and response within one agent
- Alert triage and incident-analysis visualisation
- Real-time endpoint visibility and one-click investigation
- Tracking of live attacks and lateral movements
- Rapid response with fast resolution, containment and remediation

4.6.3 Advanced Threat Protection

Grant McGregor's Advanced Threat Security service comprises a suite of advanced multi-layer anti-Malware software which provides Endpoint monitoring and threat detection. It provides both foundational security and highly advanced protection, leveraging market leading advanced threat intelligence, detection and response technology. The suite comprises an Endpoint agent which executes Endpoint scans, a detection layer and a sandbox analyser.

Detection

This defence layer operates in the pre-execution phase and features local machine learning models and advanced heuristics (which are trained to identify hacking tools, exploits and Malware obfuscation techniques) to block sophisticated threats before execution. It also detects delivery techniques and sites that host exploit kits and blocks suspicious web traffic.

The service can be configured to block at normal or permissive level while continuing to report on an aggressive level automatically, exposing early indicators of compromise. Features include:

- Protection for the Client against targeted and file-less Malware
- Blocking of attacks pre-execution with aggressive, tuneable machine learning
- Provide threat context and visibility and enhanced detection

Sandbox Analyser

This powerful layer of protection against advanced threats analyses suspicious files in depth, detonates payloads in a contained cloud-based virtual environment, analyses their behaviour and reports malicious intent. Integrated with the Endpoint agent, the sandbox analyser automatically submits suspicious files for analysis. If a malicious verdict is received from the sandbox analyser, the Endpoint agent can, if configured, automatically block the malicious file on all systems enterprise-wide immediately. Features include:

- Choice of monitor or block mode
- Manual submission of files for analysis
- Sandbox analyser's rich forensic information provides the Client with clear context to threats

4.6.4 Multi-Factor Authentication

Multi-factor authentication is widely recognised as being more inherently secure than username / password-only authentication. Choosing the correct multi-factor authentication method is critical to End User's experience. Grant McGregor offers a number of fully managed multi-factor authentication solutions.

4.6.5 Security Awareness Training

Grant McGregor's Security Awareness Training includes a number of services which are targeted at increasing End User's awareness of cyber security threats and how to mitigate them. Security Awareness Training is a recurring service under which Grant McGregor will provide:

- Access to a wide range of cyber training materials for all End Users, with automated training campaigns and scheduled email reminders
- Fully automated, configurable simulated phishing attacks, with reporting of results
- 'Virtual Risk Officer' which provides risk scores which can be reported by End User, groups of End Users or the whole organisation
- One hour consultancy per twenty End Users per quarter, to include review and maintenance of security posture and ongoing training requirements

4.6.6 Dark Web Monitoring

End User's credentials are regularly hacked on popular websites and are made available on the dark web for sale. Grant McGregor's dark web monitoring service continually scans the dark web for End User's credentials on an ongoing basis and will raise an alert if any credentials that contain the Client's domain name appear for sale, enabling the Client to take action to change any passwords that may have been the same or similar to the compromised passwords.

4.7 Advanced Email Security

4.7.1 Grant McGregor's Advanced Email Security Service uses multilayered detection techniques to defend against constantly evolving threats. Employing signature-based detection and dynamic reputation analysis, the service blocks known Malware and continually assesses local and global IP addresses to determine whether to accept email connections. The service includes an email classifier also dynamically classifies a

wide variety of emails, including impostor, phishing, Malware, spam, bulk mail, adult content and circle of trust. It separates incoming email into separate quarantines by types. Together, these features help protect the Client at the first signs of malicious activity. The service includes:

- Anti Virus
- Spam Filtering
- Outbound Mail Filtering
- Imposter Email Protection, which protects End Users from Impersonation type email attacks, for example CEO Fraud and Business Email Compromise. Grant McGregor provides a range of methods to counter such attacks
- Content Filtering, which scans emails for suspicious content and attachment types including .pdf, .exe, and .js that are often linked with malicious attacks. Content that appears to be dangerous or spam will be scored and either be quarantined or discarded, depending on its perceived risk
- Malware 'sandboxing', which provides a proactive layer of network security defence against new and advanced persistent threats. Advanced persistent threats are custom-developed targeted attacks often aimed at compromising organisations and stealing data which are designed to evade detection
- URL Defence, which analyses every URL in an email, including password protected attachments and beyond the link to inspect the landing page for malicious behaviour. Unknown links can be rewritten to offer time-of-click protection
- Data Loss Prevention, the Service enables the Client to create and automate universal policies across multiple cloud applications to control how files are shared amongst internal and external End Users

4.7.2 Email Continuity

Grant McGregor's Email Continuity Service provides an emergency inbox, instant replay of lost or deleted emails over the last 30 days and email spooling.

4.7.3 Email Archiving

Grant McGregor's Email Archiving Service provides the following:

- Capture of all sent and received emails and their attachments
- Archiving of ten years' email items and attachments
- Secure, encrypted storage, which meets all regulatory requirements
- The provision of tools for litigation hold and e-discovery
- Search and audit

4.7.4 Email Encryption

Grant McGregor's Email Encryption Service provides powerful, policy-driven encryption features which mitigate the risks associated with regulatory violations, data loss and violations of the Client's policies, while positively enabling critical business communications.

Features include:

- Automatic application of encryption, based on the Client's policies; Compliance, data loss prevention and content security policies are consistently and accurately applied
- Internal-to-internal encryption is available with the Endpoint plug-in
- Key management, backup and administration burdens are eliminated as the Email Encryption Service provides secure, cost-efficient, highly available and fully redundant key storage facilities
- Granular message control by allowing expiration of encrypted messages and the ability to revoke any individual message to any one specific individual
- One-step encrypted email delivery for mobile and Endpoint users
- Encryption of classified documents whose metadata has been marked up with a tool such as Microsoft IAM to ensure these types of documents are only view-able by recipients with the correct classification privileges
- Decryption of secure messages at the gateway between trusted partners who are both using the Email Encryption Service, which allows End Users to view encrypted messages without needing to use secure reader

The Email Encryption Service automatically and dynamically applies encryption or decryption based on the Client's policies. The Email Encryption Service provides effective data protection without administrative burdens:

- All encryption policies are centrally managed and enforced at the gateway
- The administrative overhead of key management is minimised as keys that are generated are securely stored, managed and made highly available via the Encryption Service
- The option to enable End User key management is also available, providing End Users with the ability to revoke, expire, or restore access to encrypted email messages
- All messages can be set with specific expiration based on policy. In addition, an individual message to a specific recipient can be revoked without affecting other End Users or other messages to the same recipient
- The Email Encryption Service automatically encrypts and decrypts sensitive content as required, without End Users having to use and manage complicated digital certificates or encryption keys
- Secure messaging policies are managed and enforced on an enterprise level from a single location. Once defined, enterprise encryption policies for compliance and content security are applied automatically, consistently and accurately, eliminating the risk of user error
- The Email Encryption Service enables extremely granular, per-message control over encrypted messages and policies
- Encryption can be triggered by any combination of the following parameters:
  - Regulated information
  - Confidential information through advanced document fingerprinting
  - Based on destination, for example a specific business partner or supplier, on sender or on message attributes, such as attachment type
- Messages are delivered with a TLS connection
- Inbound Email can also be decrypted at the gateway, allowing the Client's threat protection and content compliance policies to be applied to encrypted email before it is delivered to end users and ensuring that spam, malware and noncompliant messages are properly handled

5. Service Level Agreement

5.1 Grant McGregor aims to meet the following target Response and resolution times:

Issue Severity	Target Initial Response Time	Target Resolution Plan Time	Target Resolution Time
P1 – Emergency (Working Hours)	1 Working Hour	2 Working Hours	4 Working Hours
P2 – Critical, impacts whole Site	2 Working Hours	2 Working Hours	4 Working Hours
P3 – Major, impacts department	4 Working Hours	4 Working Hours	8 Working Hours
P4 – Normal, impacts one or more End Users	8 Working Hours	16 Working Hours	24 Working Hours
P5 – Nuisance Issues	8 Working Hours	16 Working Hours	80 Working Hours

5.2 Response Time Targets (Applicable Service)

5.3 If Grant McGregor fails to meet the target initial response time for P1 or P2 problems, as set out in sub-paragraph 5.1, Grant McGregor will pay a Service Credit as follows:

- For each elapsed hour or part thereof in excess of the target initial response time for P1 or P2 problems, Grant McGregor will credit 5% of the recurring monthly charge

5.4 Failure by Grant McGregor to achieve the targets set out in this paragraph 5 shall not be deemed to be a breach of this Agreement.

6. Complaint Handling

6.1 If the Client is dissatisfied with any Services-related matter, the Client should make a complaint using the following escalation path. If the complaint remains unresolved, the Client should escalate to the next level in the escalation path.

Escalation Level	Role	Contact Details
1	Service desk	0131 603 7911 servicedesk@grantmcgregor.co.uk
2	Service Desk Team Leader	0131 603 7911 daniel.taylor@grantmcgregor.co.uk
3	Service Desk Manager	0131 603 7910 paul.sinclair@grantmcgregor.co.uk

6.2 Formal complaints can be made by e-mail or telephone, and will be responded to within three Working Days.