ITRM

Supplementary Terms for the Supply of Security Services

The Company shall provide Security Services to the Client on the terms and conditions set out in the Company's General Terms and Conditions and the terms and conditions of these Supplementary Terms. All definitions set out in the General Terms and Conditions shall, unless otherwise specified below, have the same meaning when used in these Supplementary Terms.

1. SUPPLEMENTARY DEFINITIONS

1.1 'Cloud-Based Utilities' means the collection of ancillary third-party provided services, including backup, anti-Malware, and monitoring services which will be used by the Company in support of the Security Services.

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

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

1.4 '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.

1.5 'Device' means an item of IT Equipment including servers, workstations, laptop computers, tablets, mobile telephones, routers and firewalls.

1.6 'Emergency Maintenance' means any period of maintenance for which, due to reasons beyond its reasonable control, the Company is unable to provide prior notice of.

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

1.8 'Hosted Services' means Software that is hosted in a Microsoft 365 tenant and accessed by the Client remotely.

1.9 'Hours of Cover' means the times that the Service Desk is available to respond to Incidents, and is set out in the Service Schedule.

1.10 'IT Equipment' means the Devices to be covered under the terms of this Agreement including those listed on the Order and any Devices subsequently discovered by the Company's Monitoring Services.

1.11 'Monitoring Agent' means Software which is installed on the IT Equipment and / or Hosted Services by the Company which enables security monitoring and reporting.

1.12 'Monitoring Services' means the Company's services which enable the delivery of the Security Services.

1.13 'Penetration Test' means an automatic or manual check of the Client's systems configuration pertaining to cyber security which is performed by the Company.

1.14 'Security Services' means the security services described in the Service Schedule.

1.15 'Security Update' means security updates provided by third-party software and hardware vendors.

1.16 'Service Desk' means the Company's dedicated team of qualified support specialists.

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

1.18 'Software' means the software which is installed on the IT Equipment and / or Hosted Services by the Company to enable the Security Services.

1.19 'Subscription' means a subscription to subscription-based services.

2. TERM

2.1 This Agreement will be deemed to come into effect on acceptance of the Client's Order by the Company and shall run until the RFS Date (the 'Run-Up Period') and following the RFS Date for the Minimum Term as 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 one year. 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 the Company of acceptance of changes, the Agreement shall continue in force for an Additional Term;

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

3. PROVISION OF SERVICES

3.1 Security Services are provided to merely mitigate the cyber vulnerability of the IT Equipment and / or Hosted Services.

3.2 The Service Components to be provided under the terms of this Agreement are described in the Service Schedule.

3.3 Security Services will be provided by the Company remotely.

3.4 For the avoidance of doubt, Security Services do not include IT systems support, hardware maintenance or local area network support.

3.5 The Company shall use reasonable endeavours to provide the Security Services during the Hours of Cover described in the Service Schedule.

3.6 During the term of this Agreement, the Company shall be entitled to make alterations to the Configuration of the IT Equipment and / or Hosted Services. Such alterations may result in temporary disruption to the availability of the IT Equipment and / or Hosted Services and the Company will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

3.7 The Company cannot guarantee and does not warrant that the Security Services shall result in the IT Equipment and / or Hosted Services operating free from interruptions or will be free from the risk of Malware infection or other Data Security Event.

3.8 A number of the Security Services include Monitoring Services; and

3.8.1 The Company shall use reasonable endeavours to provide the Monitoring Services 24 x 7 x 365;

3.8.2 The Company cannot guarantee and does not warrant that the Monitoring Services will be free from interruptions, including:

a) Interruption of the Monitoring Services for operational reasons and temporary degradation of the quality of the Monitoring Services;

b) Interruption of the connection of the Monitoring Services to other network services provided either by the Company or a third party; and

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

4. ACCEPTABLE USE

4.1 The Client agrees to use the IT Equipment and / or Hosted Services in accordance with the provisions of this Agreement, any relevant service literature and all other reasonable instructions issued by the Company from time to time.

4.2 The Client agrees to ensure that the IT Equipment and / or Hosted Services 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 the Company's reasonable opinion brings the Company'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 and / or Hosted Services;

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, Hosted Services or Cloud-Based Utilities, 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 and / or Hosted Services 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 and / or Hosted Services.

4.4 The Client agrees to not and ensure that its End Users do not share passwords provided for access to Cloud-Based Utilities.

4.5 The Client agrees, subject to the provisions of sub-clause 10.13 of the General Terms and Conditions to indemnify the Company 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. CLIENT'S OBLIGATIONS

5.1 During the term of this Agreement, the Client shall:

5.2 Pay all agreed additional Charges levied by the Company.

5.3 Ensure that user-names, passwords and personal identification numbers are kept secure .

5.4 Accept that is the Client's sole responsibility to take all reasonable steps to prevent the introduction of Malware into the IT Equipment and / or Hosted Services.

5.5 Be solely responsible for ensuring compliance with the terms of licence of any Software that is a component of the IT Equipment and / or Hosted Services that has been provided by the Client.

5.6 Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the Security Services.

5.7 Be responsible for implementing (or requesting that the Company implements) the Company's recommendations and acknowledges if that such recommendations are not implemented, it may be impossible for the Company to provide the Service, and failure to implement the Company's recommendations will be deemed a material breach of this Agreement.

6. THE COMPANY'S OBLIGATIONS

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

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

6.2 During the Hours of Cover, make available a Service Desk that shall provide support and guidance in the use of the Services and manage the resolution of any Incidents that arise in the Security Services.

6.3 Be responsible for the licensing and installation of Monitoring Agents and all Software that the Company installs on the IT Equipment and / or Hosted Services.

6.4 Register and maintain the Client's Subscriptions to the third-party Hosted Services set out in this Agreement, subject to any service limitations set out in the Order and Service Schedule.

7. Clause Intentionally Unused

8. GENERAL

8.1 The installation of Security Updates may limit the availability of the IT Equipment and / or Hosted Services. The Company will use reasonable endeavours to schedule Security Updates to minimise disruption to the Client; and

8.1.1 The Client shall test its IT Equipment and / or Hosted Services once the Security Update has been applied to ensure it has not impacted their functionality. If a Security Update has an adverse effect on the operation of the Software, the Company will where possible remove the Security Update, in agreement with the Client;

8.2 The Company may be unable to provide prior notice of Emergency Maintenance to the Hosted Services, but will endeavour to minimise the impact of any such maintenance on the Client.

8.3 If the Company carries out work in response to an Incident reported by the Client and the Company subsequently determines that such Incident was not in the Security Services or caused by any act or omission by the Company, it shall be entitled to charge the Client at its prevailing rate.

8.4 In the event of persistent breach of clause 4.2.8, the Company shall be entitled to:

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

8.4.2 Terminate this Agreement.

8.5 If the Client suffers a Data Security Event and subsequently requests assistance from the Company, 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 the Company.

8.6 If the Client is contacted by the Company and requested to make a change to the Configuration of the IT Equipment and / or Hosted Services, it is the Client's sole responsibility to verify the identity of the requestor prior to carrying out the requested change.

8.7 The Client is responsible for the licensing of all other software, including Windows operating systems, Microsoft Office and line of business applications which have not been supplied by the Company under the terms of any other agreement between the Company and the Client.

8.8 The Client agrees not to reverse any security policy changes made by the Company without the prior written consent of the Company (such consent not to be unreasonably withheld or delayed).

8.9 The Client hereby consents to the Company and its sub-contractors and suppliers accessing the IT Equipment and Hosted Services, for the sole purpose of providing the Services; and

8.9.1 Acknowledges that during the configuration of certain Service Components, the Company, its sub-contractors and suppliers may require global administrative access to the Hosted Services.

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 Immediately by the Company in the event that it is so instructed by government or a regulatory body;

9.1.3 By the Company if it can no longer provide the Services;

9.1.4 By the Client by reason of the Company's un-remedied or repeated material breach of the terms of this Agreement;

9.1.5 By the Client if the Company or its supplier makes changes to the Services which materially adversely affect the Client (which for the avoidance of doubt, does not include changes to Charges);

9.2 The Company may terminate the provision of any Service Component on written notice in the event that its supplier of such Service Component ceases to provide the Service Component to the Company.

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

10. CHARGES AND PAYMENT

10.1 Invoices for periodic Charges shall be raised in advance of the relevant period. The invoicing period is set out on the Order.

10.2 The periodic Charges will be based on the number End Users and / or Devices set out on the Order and as added to the Client's estate from time to time and subsequently discovered by the Company's Monitoring Services.

10.3 In addition to Charges contemplated in sub-clause 10.2, the Company 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 based on the number of End Users supported at the date of notification of termination.

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

10.5 On-boarding and usage-based Charges, including Charges made for use of Services in excess of any pre-paid amounts, will be invoiced in arrears.

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

10.7 The Managed IT Services will be provided by the Company for use by the Client on a Fair Use basis. If, in the reasonable opinion of the Company, the Client's use of the Services is deemed excessive, the Company shall be entitled to charge the Client at its prevailing rate for the supply of such Services.

10.8 The Client agrees that it shall be liable for termination Charges in the event that this Agreement is terminated by:

10.8.1 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 Recurring Charges payable for the remainder of the current term, any outstanding installation Charges and the Termination Fee;

10.8.2 The Company 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 Recurring Charges payable for the remainder of the current term, any outstanding installation Charges and the Termination Fee.

10.9 If the Client terminates this Agreement at the end of the Minimum Term or any Additional Term thereafter in accordance with clause 9, the Client shall be liable to pay the Termination Fee.

10.10 The Client shall not be liable for Early Termination Charges if this Agreement is terminated by:

10.10.1 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;

10.10.2 A right of termination arises under the provisions of sub-clauses 9.1.2 to 9.1.5.

11. LIMITATIONS AND EXCLUSIONS

11.1 The following are not included under the terms of this Agreement:

11.1.1 IT policy and template design;

11.1.2 Compliance issues;

11.1.3 IT Equipment or Hosted Services support or maintenance;

11.1.4 Changes to the Configuration of the IT Equipment and / or Hosted Services other than those covered by the Security Services;

11.1.5 On-Site support;

11.1.6 Remediation, Malware removal or data restoration following a Malware attack.

11.2 The Company, if requested, may provide any of the excluded services listed above, and will charge for so doing at its prevailing rate.

12. EXCLUSION OF LIABILITY

12.1 The Client acknowledges and agrees that:

12.1.1 Any recommendations or advice provided by the Company is intended to merely 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;

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

12.2 The Client agrees that the Company shall not be liable for any actions, losses damages, judgements, legal fees, costs, fines, claims or expenses incurred by the Client or legal proceedings which are brought or threatened against the Client by a third party in the event of:

12.2.1 Any breaches by the Client of any Data Protection Legislation;

12.2.2 Any security breach of or vulnerability in the Client's systems and processes.

12.3 All Security Services are provided on an 'as is' basis, without warranty, guarantee of fitness for purpose or suitability for the Client's purpose; and

12.3.1 The Company shall not be liable for any damages or costs arising from a failure of any component of the Security Services, including failure to detect Malware, Data Security Events or the requirement for Security Updates unless such failure is caused by the negligence of the Company.

12.4 The Company 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.

12.5 Security Updates are supplied by the Company-authorised software vendors and not the Company. The Company will use reasonable endeavours to prevent a Security Update causing an adverse reaction with any particular IT Equipment and / or Hosted Services configuration, but the Company shall not be liable for any disruption resulting from the installation of Security Updates. In such circumstances, the Company's sole responsibility will be to de-install the Security Update or roll back to an appropriate restore point to resolve the issue.

12.6 The Client acknowledges and agrees that:

12.6.1 There is a small risk that Penetration Tests carried out by the Company may cause problems in the Client's IT systems, including routers and / or firewalls ceasing to function correctly and database and storage access issues;

12.6.2 The testing of the Client's IT systems for correct functioning after the Company's Penetration Tests and any necessary reconfiguration, and any associated costs shall be the Client's sole responsibility;

12.6.3 Whilst the Company warrants that it shall use reasonable care during the execution of Penetration Tests, the Company shall not be liable for any losses or damage which arise either directly or indirectly from its access to the Client's IT infrastructure.

12.7 The provisions of this clause 12 shall survive the termination of this Agreement in perpetuity.

Service Schedule

This paragraph summarises all of the security Service Components that the Company can provide. The individual Service Components to be provided to the Client under the terms of this Agreement are set out on the Order.

1. Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps is a cloud access security broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber-threats across the Client's Microsoft and third-party cloud services. Microsoft Defender for Cloud Apps natively integrates with leading Microsoft solutions and provides simple deployment, centralised management, and innovative automation capabilities, which helps the Client to:

- Discover and control the use of shadow IT: Identify the cloud-based apps and services used by the organisation, investigate usage patterns and assess the risk levels and business readiness of more than 25,000 cloud-based apps against more than 80 risks
- Protect sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real time across all cloud-based apps in the organisation
- Protect against cyber-threats and anomalies: Detect unusual behaviour across cloud-based apps to help identify ransomware, compromised users or rogue applications, analyse high-risk usage and remediate automatically to limit the risk to the organisation
- Assess the compliance of cloud-based apps used by the organisation: Assess if the organisation's cloud-based apps meet relevant compliance requirements including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data

2. Email Security and Web Filtering Services

Email Security Services provide comprehensive protection from traditional email threats including spam, Malware, large-scale phishing attacks and malicious URLs and includes the following features:

- Incorporates multiple technologies to ensure enterprise class threat detection rates with very high accuracy
- Full analysis of inbound email with optional outbound email analysis using unlimited keyword lists
- Multiple traditional signature and behaviour based anti-virus engines including static sandboxing of file attachments
- Time of click protection from malicious URLs and downloaded files in emails with the option to scan links at time of delivery
- Web filtering prevents access to harmful, offensive, inappropriate or illegal content on malicious pages or hidden deep within legitimate sites

The following services may also be provided:

- Secure Email: Provides a simple solution to sending encrypted emails to specific recipients
- Email Archiving: Provides a fully compliant archive with unlimited storage for an unlimited time
- Data Loss Protection: Monitors outbound email traffic and alert End Users to potential data breaches

3. Email Continuity

Email Continuity provides End Users with an 'Emergency Inbox' accessed via a browser if the primary email server fails.

4. Zero Trust Protection

The Company's Zero Trust Protection provides a suite of services that are designed to mitigate risk of cyber attack to the Client's IT Infrastructure.

4.1 By defining how applications can interact with each other, and by controlling what resources applications can access, such as networks, files, and registries, Zero Trust Protection helps to prevent file-less Malware and software exploits, including:

- Protecting data from malicious behaviour
- Preventing file-less Malware and limit damage from application exploits
- Defining how applications integrate with other applications
- Preventing applications from interacting with other applications, network resources, registry keys, and files
- Preventing applications from interacting with built-in tools such as PowerShell, Command Prompt and RunDLL
- Preventing built-in tools from accessing file shares

4.2 Application whitelisting has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, application whitelisting provides control over which software, scripts, executables, and libraries can run on the Client's IT Infrastructure. This approach not only stops malicious software, but it also stops other unpermitted applications from running and therefore mitigates cyber threats.

4.3 Storage protection provides an advanced storage control solution that protects information by enabling the Client to control the flow and access of data. The Client can choose what data can be accessed, or copied, and the applications, users, and Devices that can access the data. Storage control allows the Client to:

- Choose how data is accessed
- Visualise a full audit of all file access on USB, Network, and Local Hard Drives
- Restrict or deny access to external storage, including USB drives, network shares, or other devices
- Approve for a limited amount of time or permanently
- Restrict access to specific file types
- Limit access to a Device or file share based on the application
- Enforce or audit the encryption status of USB hard drives and other external storage

4.4 Elevation control enables End Users to run selected applications as a local admin and remove local admin permissions without stopping productivity. Elevation control provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their End Users, whilst allowing them to run individual applications as an administrator. Key Capabilities of Elevation control include:

- Providing complete visibility of administrative rights
- Providing the ability to approve or deny an End User's administrator access to specific applications within an organization even if the End User is not a local administrator
- End Users can request permission to elevate applications and add notes to support their requests
- Allows setting durations for how long End Users are allowed access to specific applications by granting either temporary or permanent access

5. Dark Web Credential Monitoring

End User's credentials are regularly hacked on popular websites and are made available on the dark web for sale. The Company's Dark Web Credential Monitoring service regularly scans the dark web for End User's credentials 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.

6. Security Awareness Training

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 the Company 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

7. Video Training Services

Video Training Services comprise an online portal which hosts a number of training and development videos, covering a range of technical and personal development topics. The courses will be made available to the designated End Users for the duration of this Agreement.

The Company will provide Access Credentials for the Video Training Services. The courses will be accessible to End Users via a standard web browser. Examples of the video training courses include:

- Office 365
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Personal Cyber Security
- Customer Service
- Selling Skills

8. Endpoint Protection

The Company’s Endpoint Protection service comprises a suite of advanced multi-layer anti-Malware software which provides endpoint monitoring and threat detection. The service protects against known, unknown Malware and ransomware, and file-less and Malware-free attacks. Features include:

- Full attack visibility provides details, context and history for every alert
- Automated, scripted and analyst-driven intervention capabilities enable efficient and powerful remediation
- Threat Intelligence integration immediately assesses the origin, impact and severity of threats in the environment and provides recovery guidance for decisive incident response and remediation
- Machine learning and artificial intelligence detect known and unknown Malware and ransomware
- Behaviour-based indicators of attack prevent sophisticated file-less and Malware-free attacks
- Exploit blocking stops the execution and spread of threats via un-patched vulnerabilities
- Detect and quarantine on write stops and isolates malicious files when they first appear on a host
- Industry-leading threat intelligence to actively block malicious activity
- Automated IOA remediation cleans up known artefacts left behind from blocked malicious activity

9. Endpoint Security Service

The Company’s Managed Next Generation Anti-Malware Service provides full Security Operations Centre (‘SOC’) supported Endpoint monitoring and threat detection to identify active threats and remediate attacks. Using advanced artificial intelligence and machine learning, the Company rapidly identifies and halts the most sophisticated attacks, minimising harm and reducing risk to the Client’s Endpoints. In more extreme cases such as ransomware, the SOC will roll back to restore system and data access.

The service includes containment and remediation elements, thus the Client should ensure that this service does not conflict with the provisions of any cyber-insurance policy that is held by the Client prior to subscribing to this service.

10. Automated Security Patch Management

The Company will install approved security patches for Servers, Endpoints and Hosted Services as they are made available for Microsoft-supported operating systems and applications. Where a Server or Endpoint re-boot is required to complete patch installation, this will be performed in agreement with the Client.

11. Password Management Service

The Password Management Service provides secure End User password vaults, one-click website logins and a host of other features, including:

- Credential discovery and automation
- Multifactor authentication (MFA)
- Active Directory two-way sync
- Mobile optimised access
- Password data analytics and reporting
- Password history retention
- Windows directory services control
- Custom security groups
- Temporary access rights
- Scheduled automated data exports

12. Penetration Test Service

12.1 The Company's Penetration Test Service is provided by a partner who is NCSC-certified, a member of CREST (Council of Registered Ethical Security Testers) and has over fifteen years of experience of designing and delivering penetration tests for every sector and across a vast range of technologies. Its specialist penetration testers apply stringent, innovative testing methodologies that meet the highest levels of security assurance requirements to ensure that the Client's business remains protected.

12.2 Penetration testing is a security test process that systematically tests the external facing components of the Client's IT infrastructure for weaknesses and vulnerabilities. The results provide a snapshot of the Client's IT security profile and any vulnerability together with reporting and relevant remediation advice.

13. Automated Penetration Testing Service

The Company's Automated Penetration Testing Service is an automated IT infrastructure penetration testing service that runs similar tests to those provided in a manual Penetration Test. This includes technical tasks such as host discovery, service enumeration, vulnerability analysis, exploitation, post-exploitation, privilege escalation and lateral movement. As with manual testing, the results provide a snapshot of the Client's IT security profile and any vulnerability together with reporting and relevant remediation advice.

14. Cyber Essentials Readiness Consultancy

The Company will assess the Client' security posture against a Cyber Essentials assessment questionnaire and report its results to the Client. The report will take the form of a gap analysis and will identify areas of non-compliance with the security standard which would cause a Cyber Essentials assessment to fail. If further technical assistance is required (that is, regarding making changes to the Client's systems or processes), such is not covered under the terms of this Agreement, however the Company will provide such technical assistance, chargeable at its prevailing rates, if requested.

15. Microsoft 365 Tenant Policy Management

The Company will manage, monitor and track changes of the Client's security policies on the Hosted Services. The Company provides two levels of service, ITRM Inforce Foundation and ITRM Inforce Advanced. The service to be provided under this Agreement is set out on the Order.

15.1 ITRM Inforce - Foundation includes:

15.1.1 Backup and restore Microsoft 365 settings, including:

- Endpoint Security Policies
- Conditional Access Polices
- Device Policies (Autopilot / Intune)
- Application Management Policies

15.1.2 Enhanced 365 Reporting, including:

- Licensing Type & Count

- Global Admins
- Active users and user count
- OneDrive
- Secure Score Capture & Comparisons
- Intune
- SharePoint
- MFA

15.2 ITRM Inforce - Advanced includes:

15.2.1 All of the features of ITRM Inforce – Foundation, plus:

- Security Baselines
- Change Auditing
- Baseline Enforcement
- Policy Updates

16. Firewall Management

The Company's Firewall Management service includes:

- Security Updates to firmware and software to maintain security levels
- Managing access in response to Client requests
- Changes to rules in response to Client requests
- If such functionality is available and enabled, filtering website access; allowing the Client to selectively block End User access to specified websites
- If such functionality is available and enabled, changes to setup, including unblocking websites, making exceptions for users and individual endpoints in response to Client requests

17. Backup Service for Microsoft 365 and Azure

17.1 The Company's Backup Service for Microsoft 365 and Azure 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 the Company's service, in addition to providing the Client with additional control over its data, mitigates the risk of such data loss.

17.2 The Company provides a number of backup and recovery options. The options selected are set out on the Order. Options include:

- Cloud backup at the Company's Data Centre
- Backup to a resilient backup appliance which is located at the Client's Site, which can be provided by the Company or the Client.
- Backup to the Client's nominated Data Centre

17.3 Backups can be made at image (server, virtual server or endpoint) or file / folder level.

17.4 Backups are encrypted at rest and during transmission.

17.5 The Company will back-up the Client's Microsoft 365 data based on the number of End Users and storage capacity set out on the Order; backup data is stored the Company's Data Centre.

17.6 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), if supported by the backup service subscribed to
- Contacts, tasks and calendars

17.7 Backup frequency and retention periods are set out on the Order.

17.8 The Backup and Recovery Service is fully managed by the Company.

17.9 The backup system will automatically notify the Company of backup success or failure.

17.10 Data restoration:

- Data restores will only be initiated by the Company when requested by an authorised representative of the Client
- The Company will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level) requested by the Client
- The Company will use reasonable endeavours to restore data to the location that is specified by the Client
- Restores can be made at file, mailbox, Sharepoint Site or virtual server level
- Requests for data restores will be accepted by the Company on a Fair Use basis

17.11 Whilst the Company shall execute automatic backups and monitor the performance of the backup service 24 x 7 x 365, the Company will carry out the following activities during the Hours of Cover:

- Respond to Client requests for data restores
- Respond to and investigate any Incidents that arise in the service which cannot be remediated automatically, whether raised by the Client or by the Company's Monitoring Agents

17.12 Test Data Restore

In response to requests from the Client, the Company will perform occasional test restores of backed-up data to ensure that backups are functioning correctly. This will be implemented by the Company contacting the Client to agree a test target (for example a mailbox or SharePoint Site) and carrying out the test restore at an agreed time. The Company will charge for providing Test Data Restores at its prevailing rate.

18. Service Desk

18.1 Subject to fair usage, there are no restrictions on the number of Incidents that the Client can report to the Company's Service Desk. The Service Desk provides support and assistance in the use of the Security Services, including the following:

- Management of the prompt resolution of Security Services-related Incidents within the IT Equipment and / or Hosted Services that are identified by the Client
- Remote access to facilitate Incident resolution if possible and appropriate
- Escalation management if required in the event of protracted Incident resolution
- Third-party vendor liaison where required

18.2 The Client may report Incidents by one of the following methods:

- Via the Company's web support portal: www.itrm.co.uk
- By Email: service@itrm.co.uk
- By Telephone to the Company's Service Desk: 020 8308 3310

18.3 When reporting an Incident, the Client should provide the following information:

- Name of Client and person reporting the Incident
- Contact telephone number
- Description of the Incident
- Description of actions taken prior to the Incident occurring
- Explanation of how the Incident has been diagnosed
- Any other relevant information

18.4 The Service Desk Hours of Cover are from 9am to 5pm Monday to Friday, excluding public holidays.

19. Service On-boarding

19.1 The Company shall install Software that is required to deliver the Services, on the IT Equipment and / or Hosted Services.

19.2 The Company will review and where necessary recommend or make appropriate changes to the IT Equipment's and / or Hosted Services' configurations to ensure that the Services included on the Order can be delivered effectively. This will include but is not limited to the configuration of operating system software.

19.3 Application of the latest Security Updates for operating systems, Microsoft Office and where such applications are listed on the Order, third-party applications.

19.4 The Company perform initial scans of the IT Equipment and / or Hosted Services to ensure that such is free from Malware.

20. Escalation Process

20.1 If any Incident remains unresolved, the Client should escalate using the following escalation path. If the Incident remains unresolved, the Client should escalate to the next level in the escalation path.

Escalation Level	Role	Contact Details
1	Service Desk Dispatcher	020 8308 3310
2	Dedicated Account Manager	
3	Service Delivery Manager	
4	Service Delivery Director	
5	Managing Director	