

Supplementary terms for the supply of Managed IT Services

The Services set out in these Supplementary Terms shall be supplied by NexGen Cyber to the Client on the terms and conditions set out in NexGen Cyber’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.

# SUPPLEMENTARY DEFINITIONS

‘Cloud-Based Utilities’ means the collection of ancillary third-party provided services, including backup, anti-Malware, and monitoring services which will be used by NexGen Cyber in support of the Managed IT Services.

‘Configuration’ means the configuration of the IT Equipment, including hardware, installed software and all associated settings and or parameters.

‘Data Centre’ means a remote data storage facility.

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

‘Emergency Maintenance’ means any period of maintenance for which, due to reasons beyond its reasonable control, NexGen Cyber is unable to provide prior notice of.

‘Endpoint’ means all computing devices save Servers, including desktop computers, laptop computers and mobile computing devices, which collectively form a sub-set of the IT Equipment.

‘End User’ means a user of the IT Equipment.

‘Hardware’ means IT equipment including Servers, routers, switches, desktop machines and other electronic devices.

‘Support Desk’ means NexGen Cyber’s dedicated team of qualified support specialists.

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

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

‘IT Equipment’ means Servers, Endpoints and any other electronic devices that are installed or used at the Client’s Site, which are listed on the Order and is/are to be supported under the terms of this Agreement.

‘Local Area Network’ (‘LAN’) means the network infrastructure at the Client’s Site.

‘Line of Business Application’ means the software which is installed on the IT Equipment and is provided by the Client.

‘Managed IT Services’ means IT support services set out on the Order and described in the Service Schedule.

‘Monitoring Agent’ means Software which is installed on the Client’s Server by NexGen Cyber which enables system monitoring and performance reporting.

‘Planned Maintenance’ means any period of maintenance for which NexGen Cyber provides prior notice.

‘Server’ means server equipment that is a sub-set of the IT Equipment, which are listed on the Order.

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

‘Software’ means the software which is installed on the IT Equipment, as listed on the Order.

# TERM

This Agreement will come into effect on acceptance of the Client’s Order by NexGen Cyber 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.

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.

NexGen Cyber 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:

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;

The Client notifies NexGen Cyber of acceptance of changes, the Agreement shall continue in force for an Additional Term;

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

# PROVISION OF SERVICES

Managed IT Services are provided to support the Client’s on-premise IT systems and Hosted Services. Managed IT Services will be provided by NexGen Cyber remotely and if set out on the Order, when required, visits shall be made to the Client’s Site. For the avoidance of doubt, Managed IT 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.

The Managed IT Services to be provided hereunder shall include those set out in the Order and described in the Service Schedule.

During the term of this Agreement, NexGen Cyber 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 NexGen Cyber will use reasonable endeavours to minimise such disruption and will provide as much notice as possible prior to such disruption.

NexGen Cyber cannot guarantee and does not warrant that the Managed IT Services shall result in the IT Equipment or Hosted Services operating free from interruptions or temporary degradation performance quality.

NexGen Cyber provides Cloud-Based Utilities under the terms of this Agreement; and:

NexGen Cyber shall use reasonable endeavours to provide the Cloud-Based Utilities 24 x 7 x 365;

NexGen Cyber cannot guarantee and does not warrant that the Cloud-Based Utilities will be free from interruptions, including:

1. Interruption of the Cloud-Based Utilities for operational reasons and temporary degradation of the quality of the Server Monitoring services;
2. Interruption of the network connection between the Cloud-Based Utilities and the IT Equipment; and
3. Any such interruption of the Cloud-Based Utilities referred to in this sub-clause shall not constitute a breach of this Agreement.

Although NexGen Cyber will use reasonable endeavours to ensure the accuracy and quality of the Cloud-Based Utilities, such are provided on an “as is” basis and NexGen Cyber 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.

# ACCEPTABLE USE

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 NexGen Cyber from time to time.

The Client agrees to ensure that the IT Equipment and / or Hosted Services are not used by its End Users to:

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

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;

Carry out any fraudulent, criminal or otherwise illegal activity;

In any manner which in NexGen Cyber’s reasonable opinion brings NexGen Cyber’s name into disrepute;

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

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

Falsify user information or forge addresses;

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

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

Connect to the IT Equipment 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;

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

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 NexGen Cyber.

Subject to the provisions of sub-clause 10.13 of the General Terms and Conditions, the Client shall indemnify NexGen Cyber against any third-party claims arising from the Client’s breach of the terms of this clause 4.

# CLIENT’S OBLIGATIONS

During the term of this Agreement, the Client shall:

Pay all additional Charges levied by NexGen Cyber, including those arising from usage-based components of the Services.

Use reasonable endeavours to ensure that user-names, passwords and personal identification numbers are kept secure and:

On a regular basis, change access passwords for all IT Equipment and / or Hosted Services that in the Client’s reasonable opinion may be liable to access by unauthorised persons.

Agree that in all instances where it attaches equipment that has not been provided by NexGen Cyber to the IT Equipment or Hosted Services that such equipment shall be technically compatible and conforms to any instruction issued by NexGen Cyber in relation thereto.

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 NexGen Cyber is causing disruption to the functionality of the IT Equipment, NexGen Cyber shall be entitled to:

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

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

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

Accept that is the Client’s sole responsibility to take all reasonable steps, including the implementation of anti-virus systems, firewalls and staff training to prevent the introduction of Malware into the IT Equipment or Hosted Services.

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.

Be responsible for providing external network connectivity, including access to the Public Internet, as required for the correct functioning of the IT Equipment and / or Hosted Services.

During term of this Agreement maintain a level of cyber-breach insurance cover that is appropriate to the risks associated with accidental destruction, damage, loss or disclosure of Client Data; general insurance to cover loss of or damage to the IT Equipment; and

In response to reasonable requests made by NexGen Cyber, provide evidence to show compliance with this sub-clause;

Not do or omit to do anything which would destroy or impair the legal validity of the insurance;

If the Client suffers a Data Security Event and subsequently requests assistance from NexGen Cyber, ensure that such request for assistance will not breach the terms of the insurance policy prior to requesting assistance from NexGen Cyber;

Acknowledge that insurance will not relieve the Client of any liabilities under this Agreement.

# NEXGEN CYBER’S OBLIGATIONS

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

Provide the Services set out in the Order and described in the attached Service Schedule.

During the hours of cover set out in the Order, make available a Support Desk that shall provide support and guidance in the use of the IT Equipment and / or Hosted Services and manage the resolution of all Incidents raised by the Client.

During the Hours of Cover set out in the Service Schedule or as amended in the Order, monitor the performance of the Servers.

Respond to Incidents raised by the Client and make reasonable endeavours to repair any Incident that is within the IT Equipment, Hosted Services or directly caused by NexGen Cyber, its employees, agents, subcontractors or suppliers.

Proactively respond to Incidents reported by the Monitoring Agents and make reasonable endeavours to repair any Incident that is within the IT Equipment or Hosted Services.

During the Run-Up Period, NexGen Cyber shall carry out pre-service on-boarding services as described in the Service Schedule.

# Clause Intentionally Unused

# GENERAL

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

In the event of persistent breach of clause 4.2.8, NexGen Cyber shall be entitled to:

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

Terminate this Agreement.

NexGen Cyber 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.

NexGen Cyber may be unable to provide prior notice of Emergency Maintenance to the Cloud-Based Utilities, but will endeavour to minimise the impact of any such maintenance on the Client.

If the Client suffers a Data Security Event and subsequently requests assistance from NexGen Cyber, 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 NexGen Cyber.

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

If NexGen Cyber 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.

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

The Client hereby consents to NexGen Cyber and its sub-contractors accessing the IT Equipment and Hosted Services, for the sole purpose of providing the Services.

# TERMINATION

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

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 at any time thereafter.

By the Client by giving thirty days’ notice in writing if NexGen Cyber makes changes to the Services which are materially adversely affect the Client (for the avoidance of doubt, not including changes to Charges) PROVIDED THAT such notice is given within twenty eight days of the effective date of the change(s).

By NexGen Cyber at any time if it can no longer provide the Services;

By the Client by reason of NexGen Cyber’s un-remedied or repeated breach of the terms of this Agreement.

# CHARGES AND PAYMENT

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

The periodic Charges will be based on the number End Users set out on the Order and as amended from time to time.

In addition to Charges contemplated in sub-clause 10.2, NexGen Cyber shall be entitled to charge the Client for:

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

Reasonable expenses;

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

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

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.

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

If, during the term of this Agreement the Client requires additional End Users to be added to the Services, the Client shall raise a supplementary Order to cover the additional End Users and NexGen Cyber shall promptly provide a quotation for the supply of additional Services.

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

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

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 any outstanding installation Charges;

The Client terminating this Agreement for convenience during the Run-Up Period, whereupon the Client shall be liable for all set-up costs and cancellation costs incurred by NexGen Cyber up to the date that NexGen Cyber received notice of the Client’s intention to terminate;

NexGen Cyber 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 any outstanding installation Charges.

The Client shall not be liable for termination Charges if a right of termination arises under the provisions of sub-clauses 9.1.2 to 9.1.4.

# LIMITATIONS AND EXCLUSIONS

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

This Agreement and the Services provided by NexGen Cyber do not include:

The maintenance or support of any equipment that is not listed on the Order, which for the avoidance of doubt also excludes employee-owned equipment;

Repair or replacement of any damaged IT Equipment;

The supply of any consumables;

Recovery of Client data whose loss can be reasonably attributed to accidental deletion, mis-use or negligence by the Client, where such recovery necessitates work other than recovery from the latest backup or the number of requests for such is in NexGen Cyber’s reasonable opinion, excessive;

Removal of Malware or the recovery of Client’s data that results from Malware infection where either the Client has previously failed to act on recommendations made in relation thereto by NexGen Cyber or the number of requests for such is in NexGen Cyber’s reasonable opinion, excessive;

Remediation following a cyber-breach or hack where either the Client has previously failed to act on recommendations made in relation thereto by NexGen Cyber or the number of requests for such is in NexGen Cyber’s reasonable opinion, excessive;

Remediation of issues caused by Windows 10 or 11 feature upgrades where the Client has failed to follow recommendations made in relation thereto by NexGen Cyber;

Operating system installation or re-installation where the Client has failed to follow recommendations made in relation thereto by NexGen Cyber;

Software installation;

Bare-metal restores;

Support for any Software that is not supported by its manufacturer or Line of Business Applications;

The provision of development projects;

The provision of End User or “how to” training, unless otherwise agreed and subject to fair use;

Support for internet service provider outages;

Third-party warranty claim management;

NexGen Cyber may at its sole discretion provide any of the excluded services listed in this sub-clause 11.2, and charge for the supply thereof at its prevailing rates.

Whilst NexGen Cyber’s Monitoring Agents are intended to proactively identify most system-related Incidents, NexGen Cyber does not warrant and cannot guarantee that the Monitoring Agents will identify all system-related Incidents and shall not be liable for any losses, damages or costs unless such result directly from the negligence of NexGen Cyber.

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

NexGen Cyber shall not be liable for any damage or costs resulting from a failure of an update to the antivirus or anti-Malware software or definitions, or failure to detect Malware, unless such failure is caused by the negligence of NexGen Cyber.

NexGen Cyber 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.

Patches are supplied by NexGen Cyber-authorised software vendors and not NexGen Cyber. NexGen Cyber will use reasonable endeavours to prevent a patch causing an adverse reaction with any particular machine configuration, but NexGen Cyber shall not be liable for any disruption resulting from the installation of patches. In such circumstances, NexGen Cyber’s sole responsibility will be to de-install the patch or roll back to an appropriate restore point to resolve the issue.

Service Schedule

This Service Schedule describes all of the Managed IT Services that NexGen Cyber provides. Under the terms of this Agreement, Nexgen Cyber will provide the services described in paragraphs 1 to 10 plus any additional Service Packages (as described in paragraphs 11 to 13) that are set out on the Order.

# On-boarding

Prior to commencement of the Services, NexGen Cyber will on-board the Client’s IT infrastructure:

* Review and if necessary will advise the Client of changes to the IT Equipment’s configuration that are required to ensure that the Services detailed in this Service 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
* Install Monitoring Agents, anti-Malware software and inform the Client if NexGen Cyber is unable to configure any of the IT Equipment to provide the necessary alerting and will agree a suitable alternative with the Client
* Document the Client’s IT Infrastructure’s architecture and the purpose and function of each Server, and provide the Client with a copy of the report
* Make recommendations about the data that should be included or excluded as part of a backup configuration, but is not responsible for these decisions

# Support Desk

Subject to fair usage, there are no restrictions on the number of Incidents that the Client can report to NexGen Cyber’s Support Desk. The Support Desk provides support and assistance in the use of the IT Equipment and / or Hosted Services, including the following:

* Management of the prompt resolution of Incidents within IT Equipment and / or Hosted Services that are identified by the Client
* Provision of help and guidance in the use and configuration of the IT Equipment and / or Hosted Services
* Remote access to facilitate Incident resolution if possible and appropriate
* Escalation management if required in the event of protracted Incident resolution

The Client shall report Incidents by one of the following methods:

* By email to NexGen Cyber’s Support Desk: technical@nexgencyber.co.uk
* By telephone to NexGen Cyber’s Support Desk: 0204 566 6001

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

The Support Desk Hours of Cover are 9am to 5pm Monday to Friday, excluding bank and public holidays. The Client may however send emails at any time.

NexGen Cyber will use reasonable endeavours to respond to and recover Incidents that are reported.

# Automated Infrastructure Monitoring and Maintenance 24 x 7

NexGen Cyber will install its Monitoring Agents on the Servers, Endpoints and Hosted Services set out on the Order to enable pro-active monitoring. The Monitoring Agents will monitor key aspects of system performance and will alert NexGen Cyber to any detected or potential Incidents (‘Alert’). The Monitoring Agents will monitor Server, Endpoint and Hosted Services performance 24 x 7 x 365 and automatically resolve Incidents whenever possible. NexGen Cyber shall respond to any Alerts that cannot be automatically resolved during Support 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, Endpoints and Hosted Services. NexGen Cyber 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 NexGen Cyber’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
* Remote access to diagnose and remediate Incidents
* Maintain group security policy
* Maintain End User, hardware and Software asset registers

# Automated Security Patch Management

NexGen Cyber will install approved 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.

# Routine Maintenance

NexGen Cyber will carry out periodic maintenance scans of each Server and Endpoint and remove unnecessary temporary files, system/application log files, system registry settings, and temporary internet files identified by the maintenance scan. NexGen Cyber will:

* Remove the contents of the recycle bin
* Not remove internet history, recent documents, favourites, cookies, form data or passwords unless specifically requested to do so by the Client
* Continuously review the cleanup activities necessary to provide an effective service and will provide the Client with the current list of cleanup activities within three days of such request

# User Administration

NexGen Cyber 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 fair use. If in NexGen Cyber’s reasonable opinion use of this service is excessive, NexGen Cyber will be entitled to charge the Client at its prevailing rate.

# Service Performance Reporting

NexGen Cyber will provide quarterly reports which include:

* Service metrics (Incidents raised and resolved)
* End Users and active system accounts
* Supported Hardware – asset register
* Installed supported software – asset register
* Server performance / availability
* Patch update status

# Technology Business Review Meeting

NexGen Cyber will undertake periodic Technology Business 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 Incidents with the Client
* Analysing Incidents, checking for patterns to help identify root causes
* Understanding the Client’s business requirements to determine recommendations and changes where appropriate

The frequency of the meetings will be agreed with the Client at commencement of the Agreement.

# Server Backup and Disaster Recovery

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

* Cloud-based backup with backup data held at NexGen Cyber’s EU-based Data Centre
* Backup to a resilient backup appliance which is located at the Client’s Site
* Backup to a resilient backup appliance which is located at the Client’s Site, an image of which is backed up in NexGen Cyber’s Data Centre
* Backup to a resilient backup appliance which is located at the Client’s Site with a parallel backup to NexGen Cyber’s EU-based Data Centre
* Dependent on the options selected, backups can be made at image (Server, virtual Server or Endpoint) or file / folder level
* Dependent on the options selected, Servers and / or Endpoints may be backed up

Backups are encrypted at rest and during transmission.

The Backup and Recovery Service is fully managed by NexGen Cyber.

In the event of a backup failure, NexGen Cyber’s support team will receive an alert from the backup system and will investigate the problem to identify the root cause.

Backup frequency and retention periods will be agreed on commencement of the Services.

Data restores are only initiated when requested by an authorised Client representative; and

* The recovery point objective will be no later than the time of the backup prior to the system failure that resulted in the request for restoration
* The recovery time objective will be determined by the Hours of Cover
* Data can be restored at various levels of granularity, including image, folder or file level, as requested by the Client

Disaster Recovery

In the event of the Client’s Server becoming unavailable for use, at the request of the Client, NexGen Cyber will:

* Manually (that is, the recovery mode is active-passive) spin up a disaster recovery server located at its Data Centre, where such service will be available for a number of days
* Provide temporary access to the Client’s End Users until such time as access to the Client’s Server is restored

Test Data Restore

In response to requests from the Client, NexGen Cyber will perform occasional test restores of backed-up data to ensure that backups are functioning correctly. This will be implemented by NexGen Cyber 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. NexGen Cyber will charge for providing Test Data Restores at its prevailing rate.

# Complaint Handling

If 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 | Chief Technology Officer | mhardcastle@nexgencyber.co.uk |
| 2 | Chief Executive Officer | srosemeyer@nexgencyber.co.uk |

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

Optional Service Packages

Optional Service Packages will be provided as set out on the Order.

# Business Basic Package

Business Basic Package includes all of the Services listed in paragraphs 1 to 10, plus:

Basic Security Awareness Training

Basic Security Awareness Training is based on an initial online questionnaire, which identifies individual End User’s security vulnerabilities and then provides individual tailored training programs. The service also provides:

* Customised simulated phishing campaigns which can be run quarterly
* Dark web monitoring, which checks for email addresses which include the Client’s top level domain name
* Policy management, providing customisable templates for a variety of policy areas and the management of their distribution, End User acknowledgement and periodic refresh

Password Manager

NexGen Cyber’s Password Manager provides the following functionality:

* Cloud based for maximum flexibility
* Encrypted vault
* Password generator
* Multi-platform support
* Auto-fill
* Browser extensions
* Administration tools
* Multi factor authentication

Endpoint Security

NexGen Cyber’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, NexGen Cyber 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.

This service is provided under the terms of this Agreement and additionally under the terms of business of SentinelOne.

Email Protection Service

The Email Protection Service provides cloud-based protection at the Client’s email perimeter and inside the Client’s network and organisation. The Email Protection Service includes:

* Malware scanning
* Spam filtering
* Content filtering
* Outbound filtering
* Imposter (business email compromise) protection
* Credential theft protection
* URL defence (sandboxing)
* Social media account protection

Security Monitoring and Management

NexGen Cyber will install its Monitoring Agents on the IT Equipment set out on the Order to enable pro-active monitoring for Security Threats. The Monitoring Agents will alert NexGen Cyber to any Security Threats or potential Security Threats as they arise. The Monitoring Agents will monitor Endpoints and automatically resolve potential Security Threats whenever possible. NexGen Cyber shall respond to any alerts that cannot be automatically resolved during Support Desk Hours of Cover in a manner that is appropriate to the severity of the threat, whilst aiming to minimise disruption to the availability of the IT Equipment. NexGen Cyber shall:

* Automatically detect missing updates and deploy security patches to Endpoints and Servers
* Manage software and updates distribution
* Provide remote support
* Receive alerts, run reports on available updates, processes, and configurations
* Perform maintenance on the IT Equipment, even when the End User is unavailable
* Run commands, PowerShell scripts, reboot computers, and restart services remotely as required

Backup Service for Microsoft 365 and Azure

NexGen Cyber’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 NexGen Cyber’s service, in addition to providing the Client with additional control over its data, mitigates the risk of such data loss.

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

Cloud backup at NexGen Cyber’s Data Centre

Backup to a resilient backup appliance which is located at the Client’s Site, which can be provided by NexGen Cyber or the Client.

Backup to the Client’s nominated Data Centre

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

NexGen Cyber 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 NexGen Cyber’s Data Centre.

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)

Contacts, tasks and calendars

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

The Backup and Recovery Service is fully managed by NexGen Cyber.

The backup system will automatically notify NexGen Cyber of backup success or failure.

Backups are encrypted at rest and during transmission.

Data restoration:

Data restores will only be initiated by NexGen Cyber when requested by an authorised representative of the Client

NexGen Cyber will use reasonable endeavours to restore data at the level of granularity (including image, directory or file level) requested by the Client

NexGen Cyber 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.

Whilst NexGen Cyber shall execute automatic backups and monitor the performance of the backup service 24 x 7 x 365, NexGen Cyber 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 NexGen Cyber’s Monitoring Agents

Test Data Restore

In response to requests from the Client, NexGen Cyber will perform occasional test restores of backed-up data to ensure that backups are functioning correctly. This will be implemented by NexGen Cyber 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. NexGen Cyber will charge for providing Test Data Restores at its prevailing rate.

# Business Standard Package

Business Standard Package includes all of the Services listed in paragraphs 1 to 11, plus:

Mobile Device Management

Mobile device operating system support and management is provided via a NexGen Cyber-supplied Microsoft InTune subscriptions or other NexGen Cyber-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.

Advanced Security Awareness Training

NexGen Cyber’s Advanced Security Awareness Training includes a number of services which are targeted at increasing staff awareness of cyber security threats and how to mitigate them. Security Awareness Training is a recurring service under which NexGen Cyber will provide:

* Access to a wide range of cyber training materials for all staff
* Monthly random staff phishing simulations
* Regular IT security review and reports
* Access to staff security awareness assessments
* Reporting of learner assessments, scorecards, etc
* Additionally chargeable, tailored ‘spear-phishing’ simulations can be provided at the Client’s request

Advanced Password Manager

NexGen Cyber’s Advanced Password Manager provides the following functionality:

* Cloud based for maximum flexibility
* Encrypted vault
* Password generator
* Multi-platform support
* Auto-fill
* Browser extensions
* Administration tools
* Multi factor authentication
* Single sign on support for a wide range of applications

Advanced Email Protection Service

The Advanced Email Protection Service provides cloud-based protection at the Client’s email perimeter and inside the Client’s network and organisation. The Email Protection Service includes:

* Malware scanning
* Spam filtering
* Content filtering
* Outbound filtering
* Imposter (business email compromise) protection
* Data loss prevention
* URL defence (sandboxing)
* Attachment defence (reputation-based)
* Attachment defence (sandboxing)
* Email Encryption
* Social media account protection
* Emergency inbox (30 days)
* Email spooling
* Instant replay
* Tamper-proof offsite archive
* Search and discovery
* Unlimited storage (10 year archive)

Mobile Security

NexGen IT’s Mobile Security service gives the Client direct insight into the threats that can affect its employees’ mobile devices. The service protects both Android and iOS devices and the cloud-based dashboard that provides immediate visibility and analysis of mobile-borne threats. The service works either in standalone mode or layered on a Mobile Device Management service. The service provides a privacy-friendly, lightweight security app for iOS and Android that helps to block mobile threats before they can harm the Client’s business.

Features of the service include:

* Quick and easy set up with zero-touch deployment and one-touch enrolment for MDM-managed devices.
* App and device threats that are monitored (Android) include:
	+ Malware
	+ Screen recording
	+ Leaky apps
	+ Camera/Microphone access
	+ App permission abuse
	+ OS exploits
	+ Vulnerable configuration
* Network threats that are monitored (Android & iOS) include∷
	+ Man-in-the-Middle at tacks
	+ Phishing
	+ Malicious proxies
	+ Malicious web scripts
	+ Unsecured Wi-fi
	+ Weak Wi-fi security

Security Assessment and Vulnerability Management

NexGen Cyber’s Security and Vulnerability Management service provides a number of services:

* Asset Discovery

Asset discovery uses several protocols to discover and probe network assets, and by leveraging several sources of ongoing vulnerability information, helps to detect vulnerabilities in the Client’s Endpoints.

* Active Directory Assessment

Active Directory assessments help to identify mis-configurations, weak policies and privileged user access.

* External IP Scans

External IP scans help detect open ports, protocols, and named vulnerabilities in public-facing network equipment such as web servers and firewalls.

* Compliance Scanning

Compliance scanning verifies compliance of the Client’s IT Infrastructure with a wide range of common cyber-security compliance standards that make up the foundation of a strong cyber-security strategy.

* Application Patching

Application Patching remediates the vulnerability associated with un-patched software by patching third-party Windows applications. This reduces risk exposure and helps safeguard the Client’s IT Infrastructure.

* Application Baseline

Application baseline scans the Client’s IT Infrastructure to detect inconsistencies between the installed base and the documented baseline and provides a report.

# Business Professional Package

Business Professional Package includes all of the Services listed in paragraphs 1 to 12, plus:

Mobile Device Management and Conditional Access

Mobile device operating system support and management is provided via a NexGen Cyber-supplied Microsoft InTune subscriptions or other NexGen Cyber-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
* Conditional Access for Exchange, Microsoft 365 and Microsoft 365 apps on mobile device

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

Extended Support Desk Hours of Cover

The Hours of Cover for the Support Desk are extended to 24 x 7 x 365.

Zero Trust Protection

NexGen Cyber’s Zero Trust Protection provides a suite of services that are designed to mitigate risk of cyber attack to the Client’s IT Infrastructure.

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

Whitelisting has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, 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.

Zero Trust 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, End Users, and IT Equipment 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 an Endpoint or file share based on the application

Enforce or audit the encryption status of USB hard drives and other external storage

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

Ensuring that once applications are elevated, End Users cannot jump to infiltrate connected applications within the network

Network access control provides cloud-managed Endpoint and server firewall functionality with dynamic access control lists to block unwanted network traffic. Network access control allows total control of inbound traffic to the Client’s protected IT Equipment. Key capabilities of network access control include:

The ability to configure network access to Endpoints using global and granular policies

A centralised view of Endpoint policies across the Client’s IT Infrastructure